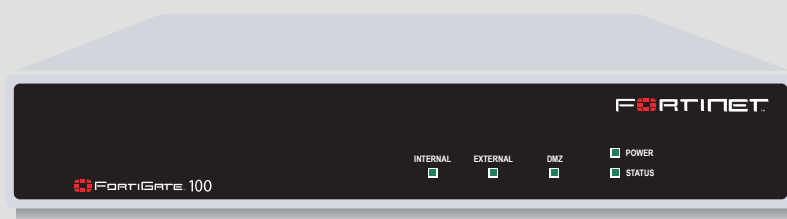


FORTINET™

FortiGate 100

Installation and Configuration Guide



FortiGate User Manual Volume 1

Version 2.50 MR2

18 August 2003

© Copyright 2003 Fortinet Inc. All rights reserved.

No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet Inc.

FortiGate-100 Installation and Configuration Guide

Version 2.50 MR2

18 August 2003

Trademarks

Products mentioned in this document are trademarks or registered trademarks of their respective holders.

Regulatory Compliance

FCC Class A Part 15 CSA/CUS

For technical support, please visit <http://www.fortinet.com>.

Send information about errors or omissions in this document or any Fortinet technical documentation to techdoc@fortinet.com.

Table of Contents

Introduction	13
Antivirus protection	13
Web content filtering	14
Email filtering	14
Firewall.....	15
NAT/Route mode	15
Transparent mode.....	16
Network intrusion detection.....	16
VPN.....	16
Secure installation, configuration, and management.....	17
Web-based manager	17
Command line interface	18
Logging and reporting	19
What's new in Version 2.50	19
System administration.....	19
Firewall.....	20
Users and authentication	20
VPN.....	20
NIDS	21
Antivirus	21
Web Filter.....	21
Email filter	21
Logging and Reporting.....	21
About this document	22
Document conventions	23
Fortinet documentation	24
Comments on Fortinet technical documentation.....	24
Customer service and technical support.....	25
 Getting started	 27
Package contents	28
Mounting	28
Powering on	29
Connecting to the web-based manager	30
Connecting to the command line interface (CLI).....	31
Factory default FortiGate configuration settings	31
Factory default NAT/Route mode network configuration	32
Factory default Transparent mode network configuration.....	33
Factory default firewall configuration	33
Factory default content profiles.....	34

Planning your FortiGate configuration	37
NAT/Route mode	37
NAT/Route mode with multiple external network connections	38
Transparent mode	38
Configuration options	39
FortiGate model maximum values matrix	40
Next steps	41
NAT/Route mode installation	43
Preparing to configure NAT/Route mode	43
Advanced NAT/Route mode settings	44
DMZ interface	44
Using the setup wizard	45
Starting the setup wizard	45
Reconnecting to the web-based manager	45
Using the command line interface	45
Configuring the FortiGate unit to operate in NAT/Route mode	45
Connecting the FortiGate unit to your networks	47
Configuring your networks	48
Completing the configuration	48
Configuring the DMZ interface	48
Setting the date and time	48
Enabling antivirus protection	49
Registering your FortiGate	49
Configuring virus and attack definition updates	49
Configuration example: Multiple connections to the Internet	49
Configuring Ping servers	51
Destination based routing examples	51
Policy routing examples	54
Firewall policy example	55
Transparent mode installation	57
Preparing to configure Transparent mode	57
Using the setup wizard	58
Changing to Transparent mode	58
Starting the setup wizard	58
Reconnecting to the web-based manager	58
Using the command line interface	59
Changing to Transparent mode	59
Configuring the Transparent mode management IP address	59
Configure the Transparent mode default gateway	59
Connecting the FortiGate unit to your networks	60

Completing the configuration	61
Setting the date and time	61
Enabling antivirus protection	61
Registering your FortiGate	61
Configuring virus and attack definition updates	61
Transparent mode configuration examples	62
Default routes and static routes	62
Example default route to an external network	63
Example static route to an external destination	64
Example static route to an internal destination	67
System status	69
Changing the FortiGate host name	70
Changing the FortiGate firmware	70
Upgrade to a new firmware version	71
Revert to a previous firmware version	72
Install a firmware image from a system reboot using the CLI	75
Test a new firmware image before installing it	77
Installing and using a backup firmware image	79
Manual virus definition updates	82
Manual attack definition updates	83
Displaying the FortiGate serial number	83
Displaying the FortiGate up time	83
Backing up system settings	83
Restoring system settings	84
Restoring system settings to factory defaults	84
Changing to Transparent mode	85
Changing to NAT/Route mode	85
Restarting the FortiGate unit	85
Shutting down the FortiGate unit	86
System status	86
Viewing CPU and memory status	86
Viewing sessions and network status	87
Viewing virus and intrusions status	88
Session list	89

Virus and attack definitions updates and registration 91

Updating antivirus and attack definitions	91
Connecting to the FortiResponse Distribution Network	92
Configuring scheduled updates	93
Configuring update logging	94
Adding an override server	95
Manually updating antivirus and attack definitions	95
Configuring push updates	95
Push updates through a NAT device	96
Scheduled updates through a proxy server	100
Registering FortiGate units	101
FortiCare Service Contracts	101
Registering the FortiGate unit	102
Updating registration information	104
Recovering a lost Fortinet support password	104
Viewing the list of registered FortiGate units	104
Registering a new FortiGate unit	105
Adding or changing a FortiCare Support Contract number	105
Changing your Fortinet support password	106
Changing your contact information or security question	106
Downloading virus and attack definitions updates	106
Registering a FortiGate unit after an RMA	107

Network configuration 109

Configuring interfaces	109
Viewing the interface list	110
Bringing up an interface	110
Changing an interface static IP address	110
Adding a secondary IP address to an interface	110
Adding a ping server to an interface	111
Controlling management access to an interface	111
Configuring traffic logging for connections to an interface	112
Configuring the external interface with a static IP address	112
Configuring the external interface for DHCP	112
Configuring the external interface for PPPoE	113
Changing the external interface MTU size to improve network performance	113
Configuring the management interface (Transparent mode)	114
Adding DNS server IP addresses	115

Configuring routing.....	115
Adding a default route	116
Adding destination-based routes to the routing table.....	116
Adding routes in Transparent mode.....	117
Configuring the routing table.....	118
Policy routing	118
Providing DHCP services to your internal network	119
RIP configuration	121
RIP settings.....	122
Configuring RIP for FortiGate interfaces.....	124
Adding RIP neighbors	125
Adding RIP filters	126
Adding a single RIP filter.....	126
Adding a RIP filter list.....	127
Adding a neighbors filter	128
Adding a routes filter	128
System configuration	129
Setting system date and time.....	129
Changing web-based manager options	130
Adding and editing administrator accounts	132
Adding new administrator accounts	132
Editing administrator accounts	133
Configuring SNMP	134
Configuring the FortiGate unit for SNMP monitoring	134
Configuring FortiGate SNMP support	134
FortiGate MIBs.....	135
FortiGate traps	136
Customizing replacement messages.....	136
Customizing replacement messages	137
Customizing alert emails	138
Firewall configuration.....	141
Default firewall configuration.....	142
Addresses	142
Services	143
Schedules	143
Content profiles.....	143
Adding firewall policies.....	144
Firewall policy options.....	145

Configuring policy lists	149
Policy matching in detail	149
Changing the order of policies in a policy list	149
Enabling and disabling policies	150
Addresses	150
Adding addresses	151
Editing addresses	152
Deleting addresses	152
Organizing addresses into address groups	152
Services	153
Predefined services	153
Providing access to custom services	156
Grouping services	156
Schedules	157
Creating one-time schedules	158
Creating recurring schedules	158
Adding a schedule to a policy	159
Virtual IPs.....	160
Adding static NAT virtual IPs	160
Adding port forwarding virtual IPs	161
Adding policies with virtual IPs.....	163
IP pools	164
Adding an IP pool.....	164
IP Pools for firewall policies that use fixed ports	165
IP pools and dynamic NAT	165
IP/MAC binding	166
Configuring IP/MAC binding for packets going through the firewall	166
Configuring IP/MAC binding for packets going to the firewall	167
Adding IP/MAC addresses	167
Viewing the dynamic IP/MAC list	168
Enabling IP/MAC binding	168
Content profiles.....	169
Default content profiles	170
Adding a content profile	170
Adding a content profile to a policy	171
Users and authentication	173
Setting authentication timeout.....	174
Adding user names and configuring authentication	174
Adding user names and configuring authentication	174
Deleting user names from the internal database	175
Configuring RADIUS support.....	176
Adding RADIUS servers	176
Deleting RADIUS servers	176

Configuring LDAP support	177
Adding LDAP servers.....	177
Deleting LDAP servers.....	178
Configuring user groups.....	179
Adding user groups	179
Deleting user groups.....	180
IPSec VPN.....	181
Key management.....	182
Manual Keys	182
Automatic Internet Key Exchange (AutoIKE) with pre-shared keys or certificates	182
Manual key IPSec VPNs.....	183
General configuration steps for a manual key VPN	183
Adding a manual key VPN tunnel	183
AutoIKE IPSec VPNs.....	185
General configuration steps for an AutoIKE VPN	185
Adding a phase 1 configuration for an AutoIKE VPN.....	185
Adding a phase 2 configuration for an AutoIKE VPN.....	189
Managing digital certificates.....	191
Obtaining a signed local certificate	191
Obtaining a CA certificate	195
Configuring encrypt policies.....	196
Adding a source address	197
Adding a destination address.....	197
Adding an encrypt policy	197
IPSec VPN concentrators	199
VPN concentrator (hub) general configuration steps	199
Adding a VPN concentrator	201
VPN spoke general configuration steps	202
Redundant IPSec VPNs.....	203
Configuring redundant IPSec VPN	203
Monitoring and Troubleshooting VPNs	205
Viewing VPN tunnel status.....	205
Viewing dialup VPN connection status	205
Testing a VPN.....	206
PPTP and L2TP VPN.....	207
Configuring PPTP	207
Configuring the FortiGate unit as a PPTP gateway	208
Configuring a Windows 98 client for PPTP	210
Configuring a Windows 2000 client for PPTP	211
Configuring a Windows XP client for PPTP	212

Configuring L2TP	213
Configuring the FortiGate unit as a L2TP gateway	214
Configuring a Windows 2000 client for L2TP	217
Configuring a Windows XP client for L2TP	218
Network Intrusion Detection System (NIDS)	221
Detecting attacks	221
Selecting the interfaces to monitor	222
Disabling the NIDS	222
Configuring checksum verification	222
Viewing the signature list	223
Viewing attack descriptions	223
Enabling and disabling NIDS attack signatures	224
Adding user-defined signatures	224
Preventing attacks	225
Enabling NIDS attack prevention	225
Enabling NIDS attack prevention signatures	226
Setting signature threshold values	226
Configuring synflood signature values	228
Logging attacks	228
Logging attack messages to the attack log	228
Reducing the number of NIDS attack log and email messages	229
Antivirus protection	231
General configuration steps	231
Antivirus scanning	232
File blocking	233
Blocking files in firewall traffic	233
Adding file patterns to block	233
Blocking oversized files and emails	234
Configuring limits for oversized files and email	234
Exempting fragmented email from blocking	234
Viewing the virus list	234
Web filtering	235
General configuration steps	235
Content blocking	236
Adding words and phrases to the banned word list	236
URL blocking	237
Using the FortiGate web filter	237
Using the Cerberian web filter	240
Script filtering	242
Enabling the script filter	242
Selecting script filter options	242

Exempt URL list	243
Adding URLs to the exempt URL list	243
Email filter.....	245
General configuration steps	245
Email banned word list.....	246
Adding words and phrases to the banned word list	246
Email block list	247
Adding address patterns to the email block list.....	247
Email exempt list.....	247
Adding address patterns to the email exempt list	248
Adding a subject tag	248
Logging and reporting.....	249
Recording logs	249
Recording logs on a remote computer	250
Recording logs on a NetIQ WebTrends server	250
Recording logs in system memory	251
Filtering log messages	251
Configuring traffic logging	253
Enabling traffic logging.....	253
Configuring traffic filter settings.....	254
Adding traffic filter entries	254
Viewing logs saved to memory	255
Viewing logs.....	255
Searching logs	256
Configuring alert email.....	256
Adding alert email addresses.....	256
Testing alert email.....	257
Enabling alert email	257
Glossary	259
Index	263



Introduction

The FortiGate Antivirus Firewall supports network-based deployment of application-level services—including antivirus protection and full-scan content filtering. FortiGate Antivirus Firewalls improve network security, reduce network misuse and abuse, and help you use communications resources more efficiently without compromising the performance of your network. FortiGate Antivirus Firewalls are ICSA-certified for firewall, IPSec and antivirus services.

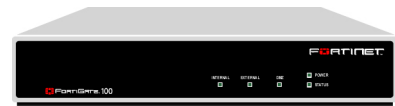
Your FortiGate Antivirus Firewall is a dedicated easily managed security device that delivers a full suite of capabilities that include:

- application-level services such as virus protection and content filtering,
- network-level services such as firewall, intrusion detection, VPN, and traffic shaping.

Your FortiGate Antivirus Firewall employs Fortinet's Accelerated Behavior and Content Analysis System (ABACAS™) technology, which leverages breakthroughs in chip design, networking, security, and content analysis. The unique ASIC-based architecture analyzes content and behavior in real-time, enabling key applications to be deployed right at the network edge where they are most effective at protecting your networks. The FortiGate series complements existing solutions, such as host-based antivirus protection, and enables new applications and services while greatly lowering costs for equipment, administration and maintenance.

The FortiGate-100 model is an easy-to-deploy and easy-to-administer solution that delivers exceptional value and performance for small office, home office, and branch office applications. The

FortiGate installation wizard guides users through a simple process that enables most installations to be up and running in minutes.



Antivirus protection

FortiGate ICSA-certified antivirus protection virus scans web (HTTP), file transfer (FTP), and email (SMTP, POP3, and IMAP) content as it passes through the FortiGate. If a virus is found, antivirus protection removes the file containing the virus from the content stream and forwards a replacement message to the intended recipient.

For extra protection, you also configure antivirus protection to block files of specified file types from passing through the FortiGate unit. You can use the feature to stop files that may contain new viruses.

If the FortiGate unit contains a hard disk, infected or blocked files can be quarantined. The FortiGate administrator can download quarantined files, so that they can be virus scanned, cleaned, and forwarded to the intended recipient. You can also configure the FortiGate unit to automatically delete quarantined files after a specified time period.

The FortiGate unit can send email alerts to system administrators when it detects and removes a virus from a content stream. The web and email content can be in normal network traffic or in encrypted IPSec VPN traffic.

ICSA Labs has certified that FortiGate Antivirus Firewalls:

- detect 100% of the viruses listed in the current In The Wild List (www.wildlist.org),
- detect viruses in compressed files using the PKZip format,
- detect viruses in e-mail that has been encoded using uuencode format,
- detect viruses in e-mail that has been encoded using MIME encoding,
- log all actions taken while scanning.

Web content filtering

FortiGate web content filtering can be configured to scan all HTTP content protocol streams for URLs or for web page content. If a match is found between a URL on the URL block list, or if a web page is found to contain a word or phrase in the content block list, the FortiGate blocks the web page. The blocked web page is replaced with a message that you can edit using the FortiGate web-based manager.

You can configure URL blocking to block all or just some of the pages on a web site. Using this feature you can deny access to parts of a web site without denying access to it completely.

To prevent unintentional blocking of legitimate web pages, you can add URLs to an Exempt List that overrides the URL blocking and content blocking lists.

Web content filtering also includes a script filter feature that can be configured to block unsecure web content such as Java Applets, Cookies, and ActiveX.

You can also use the Cerberian URL blocking to block unwanted URLs.

Email filtering

FortiGate Email filtering can be configured to scan all IMAP and POP3 email content for unwanted senders or for unwanted content. If a match is found between a sender address pattern on the Email block list, or if an email is found to contain a word or phrase in the banned word list, the FortiGate adds a Email tag to subject line of the email. Receivers can then use their mail client software to filter messages based on the Email tag.

You can configure Email blocking to tag email from all or some senders within organizations that are known to send spam email. To prevent unintentional tagging of email from legitimate senders, you can add sender address patterns to an exempt list that overrides the email block and banned word lists.

Firewall

The FortiGate ICSA-certified firewall protects your computer networks from the hostile environment of the Internet. ICSA has granted FortiGate firewalls version 4.0 firewall certification, providing assurance that FortiGate firewalls successfully screen for and secure corporate networks against a wide range of threats from public or other untrusted networks.

After basic installation of the FortiGate unit, the firewall allows users on the protected network to access the Internet while blocking Internet access to internal networks. You can modify this firewall configuration to place controls on access to the Internet from the protected networks and to allow controlled access to internal networks.

FortiGate policies include a complete range of options that:

- control all incoming and outgoing network traffic,
- control encrypted VPN traffic,
- apply antivirus protection and web content filtering,
- block or allow access for all policy options,
- control when individual policies are in effect,
- accept or deny traffic to and from individual addresses,
- control standard and user defined network services individually or in groups,
- require users to authenticate before gaining access,
- include traffic shaping to set access priorities and guarantee or limit bandwidth for each policy,
- include logging to track connections for individual policies,
- include Network address translation (NAT) mode and Route mode policies,
- include Mixed NAT and Route mode policies.

The FortiGate firewall can operate in NAT/Route mode or Transparent mode.

NAT/Route mode

In NAT/Route mode, you can create NAT mode policies and Route mode policies.

- NAT mode policies use network address translation to hide the addresses in a more secure network from users in a less secure network.
- Route mode policies accept or deny connections between networks without performing address translation.

Transparent mode

Transparent mode provides the same basic firewall protection as NAT mode. Packets received by the FortiGate unit are intelligently forwarded or blocked according to firewall policies. The FortiGate unit can be inserted in your network at any point without the need to make changes to your network or any of its components. However, VPN and some advanced firewall features are only available in NAT/Route mode.

Network intrusion detection

The FortiGate Network Intrusion Detection System (NIDS) is a real-time network intrusion detection sensor that detects and prevents a wide variety of suspicious network activity. NIDS detection uses attack signatures to identify over 1000 attacks. You can enable and disable the attacks that the NIDS detects. You can also write your own user-defined detection attack signatures.

NIDS prevention detects and prevents many common denial of service and packet-based attacks. You can enable and disable prevention attack signatures and customize attack signature thresholds and other parameters.

To notify system administrators of the attack, the NIDS records the attack and any suspicious traffic to the attack log and can be configured to send alert emails.

Fortinet updates NIDS attack definitions periodically. You can download and install updated attack definitions manually, or you can configure the FortiGate to automatically check for and download attack definition updates.

VPN

Using FortiGate virtual private networking (VPN), you can provide a secure connection between widely separated office networks or securely link telecommuters or travellers to an office network.

FortiGate VPN features include the following:

- Industry standard and ICSA-certified IPSec VPN including:
 - IPSec, ESP security in tunnel mode,
 - DES, 3DES (triple-DES), and AES hardware accelerated encryption,
 - HMAC MD5 and HMAC SHA1 authentication and data integrity,
 - AutoIKE key based on pre-shared key tunnels,
 - IPSec VPN using local or CA certificates,
 - Manual Keys tunnels,
 - Diffie-Hellman groups 1, 2, and 5,
 - Aggressive and Main Mode,
 - Replay Detection,
 - Perfect Forward Secrecy,
 - XAuth authentication,
 - Dead peer detection.

- PPTP for easy connectivity with the VPN standard supported by the most popular operating systems.
- L2TP for easy connectivity with a more secure VPN standard also supported by many popular operating systems.
- Firewall policy based control of IPSec VPN traffic.
- IPSec NAT traversal so that remote IPSec VPN gateways or clients behind a NAT can connect to an IPSec VPN tunnel.
- VPN hub and spoke using a VPN concentrator to allow VPN traffic to pass from one tunnel to another tunnel through the FortiGate unit.
- IPSec Redundancy to create a redundant AutoIKE key IPSec VPN connection to a remote network.

Secure installation, configuration, and management

Installation is quick and simple. The first time you turn on the FortiGate unit, it is already configured with default IP addresses and security policies. Connect to the web-based manager, set the operating mode, and use the setup wizard to customize FortiGate IP addresses for your network, and the FortiGate unit is set to protect your network. You can then use the web-based manager to customize advanced FortiGate features to meet your needs.

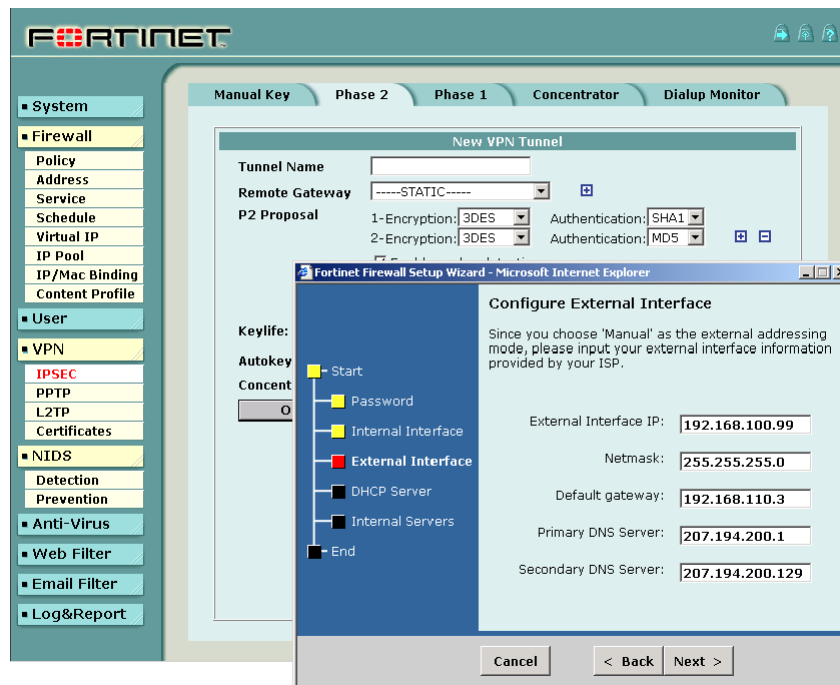
You can also create a basic configuration using the FortiGate command line interface (CLI).

Web-based manager

Using HTTP or a secure HTTPS connection from any computer running Internet Explorer, you can configure and manage the FortiGate unit. The web-based manager supports multiple languages. You can configure the FortiGate unit for HTTP and HTTPS administration from any FortiGate interface.

You can use the web-based manager for most FortiGate configuration settings. You can also use the web-based manager to monitor the status of the FortiGate unit. Configuration changes made with the web-based manager are effective immediately without the need to reset the firewall or interrupt service. Once a satisfactory configuration has been established, it can be downloaded and saved. The saved configuration can be restored at any time.

Figure 1: The FortiGate web-based manager and setup wizard



Command line interface

You can access the FortiGate command line interface (CLI) by connecting a management computer serial port to the FortiGate RS-232 serial Console connector. You can also use Telnet or a secure SSH connection to connect to the CLI from any network connected to the FortiGate, including the Internet.

The CLI supports the same configuration and monitoring functionality as the web-based manager. In addition, you can use the CLI for advanced configuration options not available from the web-based manager. This *Installation and Configuration Guide* contains information about basic and advanced CLI commands. You can find a more complete description of connecting to and using the FortiGate CLI in the *FortiGate CLI Reference Guide*.

Logging and reporting

The FortiGate supports logging of various categories of traffic and of configuration changes. You can configure logging to:

- report traffic that connects to the firewall,
- report network services used,
- report traffic permitted by firewall policies,
- report traffic that was denied by firewall policies,
- report events such as configuration changes and other management events, IPSec tunnel negotiation, virus detection, attacks, and web page blocking,
- report attacks detected by the NIDS,
- send alert email to system administrators to report virus incidents, intrusions, and firewall or VPN events or violations.

Logs can be sent to a remote syslog server or to a WebTrends NetIQ Security Reporting Center and Firewall Suite server using the WebTrends enhanced log format. Some models can also save logs to an optional internal hard drive. If a hard drive is not installed, you can configure most FortiGates to log the most recent events and attacks detected by the NIDS to shared system memory.

What's new in Version 2.50

This section presents a brief summary of some of the new features in FortiOS v2.50:

System administration

- Improved graphical FortiGate system health monitoring that includes CPU and memory usage, session number and network bandwidth usage, and the number of viruses and intrusions detected. See [“System status” on page 86](#).
- Revised antivirus and attack definition update functionality that connects to a new version of the FortiResponse Distribution network. Updates can now be scheduled hourly and the System > Update page displays more information about the current update status. See [“Updating antivirus and attack definitions” on page 91](#).
- Direct connection to the Fortinet tech support web page from the web-based manager. You can register your FortiGate unit and get access to other technical support resources. See [“Registering FortiGate units” on page 101](#).

Network configuration

- New interface configuration options. See [“Configuring interfaces” on page 109](#).
 - Ping server and dead gateway detection for all interfaces.
 - HTTP and Telnet administrative access to any interface.
 - Secondary IP addresses for all FortiGate interfaces.

Routing

- Simplified direction-based routing configuration.
- Advanced policy routing (CLI only).

DHCP server

- Addition of a WINS server to DHCP configuration.
- Reserve IP/MAC pair combinations for DHCP servers (CLI only).

RIP

- New RIP v1 and v2 functionality. See [“RIP configuration” on page 121](#).

SNMP

- SNMP v1 and v2 support.
- Support for RFC 1213 and RFC 2665
- Monitoring of all FortiGate configuration and functionality
- See [“Configuring SNMP” on page 134](#)

Replacement messages

You can customize messages sent by the FortiGate unit:

- When a virus is detected,
- When a file is blocked,
- When a fragmented email is blocked
- When an alert email is sent

See [“Customizing replacement messages” on page 136](#).

Firewall

- The firewall default configuration has changed. See [“Default firewall configuration” on page 142](#).
- Add virtual IPs to all interfaces. See [“Virtual IPs” on page 160](#).
- Add content profiles to firewall policies to configure blocking, scanning, quarantine, web content blocking, and email filtering. See [“Content profiles” on page 169](#).

Users and authentication

- LDAP authentication. See [“Configuring LDAP support” on page 177](#).

VPN

See the *FortiGate VPN Guide* for a complete description of FortiGate VPN functionality. New features include:

- Phase 1
 - AES encryption
 - Certificates
 - Advanced options including Dialup Group, Peer, XAUTH, NAT Traversal, DPD
- Phase 2
 - AES encryption
- Encryption policies select service
- Generate and import local certificates
- Import CA certificates

NIDS

See the *FortiGate NIDS Guide* for a complete description of FortiGate NIDS functionality. New features include:

- Attack detection signature groups
- User-configuration attack prevention
- Monitor multiple interfaces for attacks
- User-defined attack detection signatures

Antivirus

See the *FortiGate Content Protection Guide* for a complete description of FortiGate antivirus functionality. New features include:

- Content profiles
- Blocking oversized files

Web Filter

See the *FortiGate Content Protection Guide* for a complete description of FortiGate web filtering functionality. New features include:

- Cerberian URL Filtering

Email filter

See the *FortiGate Content Protection Guide* for a complete description of FortiGate email filtering functionality.

Logging and Reporting

See the *FortiGate Logging and Message Reference Guide* for a complete description of FortiGate logging.

- Log to remote host CSV format
- Log message levels: Emergency, Alert, critical, error, Warning, notification, information
- Log level policies
- Traffic log filter
- New antivirus, web filter, and email filter logs
- Alert email supports authentication
- Suppress email flooding
- Extended WebTrends support for graphing activity

About this document

This installation and configuration guide describes how to install and configure the FortiGate-100. This document contains the following information:

- [Getting started](#) describes unpacking, mounting, and powering on the FortiGate.
- [NAT/Route mode installation](#) describes how to install the FortiGate if you are planning on running it in NAT/Route mode.
- [Transparent mode installation](#) describes how to install the FortiGate if you are planning on running it in Transparent mode.
- [System status](#) describes how to view the current status of your FortiGate unit and related status procedures including installing updated FortiGate firmware, backing up and restoring system settings, and switching between Transparent and NAT/Route mode.
- [Virus and attack definitions updates and registration](#) describes configuring automatic virus and attack definition updates. This chapter also contains procedures for connecting to the FortiGate tech support webs site and for registering your FortiGate unit.
- [Network configuration](#) describes configuring interfaces, configuring routing, and configuring the FortiGate as a DHCP server for your internal network.
- [RIP configuration](#) describes the FortiGate RIP2 implementation and how to configure RIP settings.
- [System configuration](#) describes system administration tasks available from the System > Config web-based manager pages. This chapter describes setting system time, adding and changed administrative users, configuring SNMP, and editing replacement messages.
- [Firewall configuration](#) describes how to configure firewall policies to control traffic through the FortiGate unit and apply content protection profiles to content traffic.
- [Users and authentication](#) describes how to add user names to the FortiGate user database and how to configure the FortiGate to connect to a RADIUS server to authenticate users.
- [IPSec VPN](#) describes how to configure FortiGate IPSec VPN.
- [PPTP and L2TP VPN](#) describes how to configure PPTP and L2TP VPNs between the FortiGate and a windows client.
- [Network Intrusion Detection System \(NIDS\)](#) describes how to configure the FortiGate NIDS to detect and prevent network attacks.
- [Antivirus protection](#) describes how use the FortiGate to protect your network from viruses and worms.
- [Web filtering](#) describes how to configure web content filtering to prevent unwanted Web content from passing through the FortiGate.
- [Email filter](#) describes how to configure email filtering to screen unwanted email content.
- [Logging and reporting](#) describes how to configure logging and alert email to track activity through the FortiGate.
- The [Glossary](#) defines many of the terms used in this document.

Document conventions

This guide uses the following conventions to describe CLI command syntax.

- angle brackets < > to indicate variable keywords

For example:

```
execute restore config <filename_str>
```

You enter `restore config myfile.bak`

<xxx_str> indicates an ASCII string variable keyword.

<xxx_integer> indicates an integer variable keyword.

<xxx_ip> indicates an IP address variable keyword.

- vertical bar and curly brackets { | } to separate alternative, mutually exclusive required keywords

For example:

```
set system opmode {nat | transparent}
```

You can enter `set system opmode nat` or `set system opmode transparent`

- square brackets [] to indicate that a keyword is optional

For example:

```
get firewall ipmacbinding [dhcpiipmac]
```

You can enter `get firewall ipmacbinding` or
`get firewall ipmacbinding dhcpiipmac`

Fortinet documentation

Information about FortiGate products is available from the following FortiGate User Manual volumes:

- *Volume 1: FortiGate Installation and Configuration Guide*
Describes installation and basic configuration for the FortiGate unit. Also describes how to use FortiGate firewall policies to control traffic flow through the FortiGate unit and how to use firewall policies to apply antivirus protection, web content filtering, and email filtering to HTTP, FTP and email content passing through the FortiGate unit.
- *Volume 2: FortiGate VPN Guide*
Contains in-depth information about FortiGate IPSec VPN using certificates, pre-shared keys and manual keys for encryption. Also contains basic configuration information for the Fortinet Remote VPN Client, detailed configuration information for FortiGate PPTP and L2TP VPN, and VPN configuration examples.
- *Volume 3: FortiGate Content Protection Guide*
Describes how to configure antivirus protection, web content filtering, and email filtering to protect content as it passes through the FortiGate unit.
- *Volume 4: FortiGate NIDS Guide*
Describes how to configure the FortiGate NIDS to detect and protect the FortiGate unit from network-based attacks.
- *Volume 5: FortiGate Logging and Message Reference Guide*
Describes how to configure FortiGate logging and alert email. Also contains the FortiGate log message reference.
- *Volume 6: FortiGate CLI Reference Guide*
Describes the FortiGate CLI and contains a reference to all FortiGate CLI commands.

The FortiGate online help also contains procedures for using the FortiGate web-based manager to configure and manage your FortiGate unit.

Comments on Fortinet technical documentation

You can send information about errors or omissions in this document or any Fortinet technical documentation to techdoc@fortinet.com.

Customer service and technical support

For antivirus and attack definition updates, firmware updates, updated product documentation, technical support information, and other resources, please visit the Fortinet technical support web site at <http://support.fortinet.com>.

You can also register FortiGate Antivirus Firewalls from <http://support.fortinet.com> and modify your registration information at any time.

Fortinet email support is available from the following addresses:

amer_support@fortinet.com	For customers in the United States, Canada, Mexico, Latin America and South America.
apac_support@fortinet.com	For customers in Japan, Korea, China, Hong Kong, Singapore, Malaysia, all other Asian countries, and Australia.
eu_support@fortinet.com	For customers in the United Kingdom, Scandinavia, Mainland Europe, Africa, and the Middle East.

For information on Fortinet telephone support, see <http://support.fortinet.com>.

When requesting technical support, please provide the following information:

- Your name
- Company name
- Location
- Email address
- Telephone number
- FortiGate unit serial number
- FortiGate model
- FortiGate FortiOS firmware version
- Detailed description of the problem



Getting started

This chapter describes unpacking, setting up, and powering on your FortiGate Antivirus Firewall. When you have completed the procedures in this chapter, you can proceed to one of the following:

- If you are going to operate the FortiGate unit in NAT/Route mode, go to [“NAT/Route mode installation” on page 43](#).
- If you are going to operate the FortiGate unit in Transparent mode, go to [“Transparent mode installation” on page 57](#).

This chapter describes:

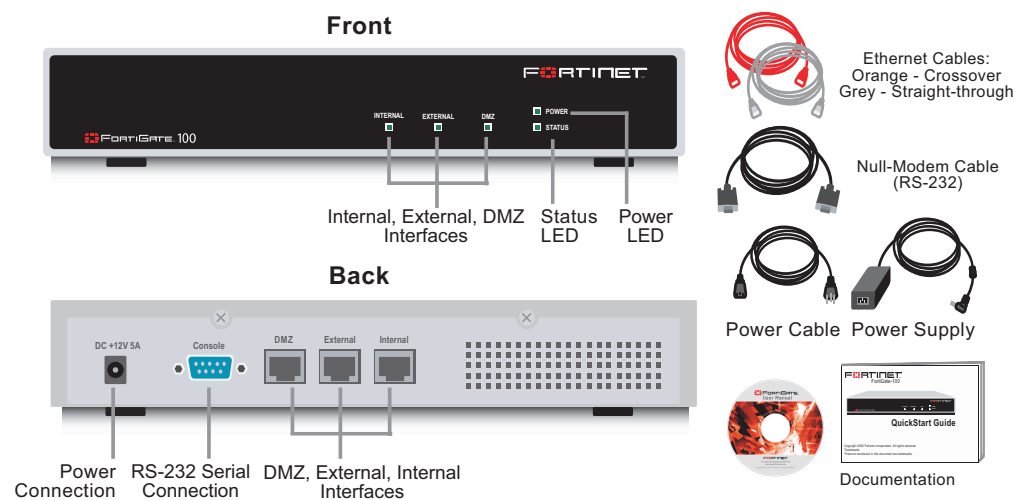
- [Package contents](#)
- [Mounting](#)
- [Powering on](#)
- [Connecting to the web-based manager](#)
- [Connecting to the command line interface \(CLI\)](#)
- [Factory default FortiGate configuration settings](#)
- [Planning your FortiGate configuration](#)
- [FortiGate model maximum values matrix](#)
- [Next steps](#)

Package contents

The FortiGate-100 package contains the following items:

- FortiGate-100 Antivirus Firewall
- one orange crossover ethernet cable
- one gray regular ethernet cable
- one null modem cable
- FortiGate-100 Quick Start Guide
- CD containing the FortiGate user documentation
- one power cable and AC adapter

Figure 2: FortiGate-100 package contents



Mounting

The FortiGate-100 unit can be installed on any stable surface. Make sure that the appliance has at least 1.5 in. (3.75 cm) of clearance on each side to allow for adequate air flow and cooling.

Dimensions

- 10.25 x 6.13 x 1.75 in. (26 x 15.6 x 4.5 cm)

Weight

- 1.75 lb. (0.8 kg)

Power requirements

- DC input voltage: 12 V
- DC input current: 5 A

Environmental specifications

- Operating temperature: 32 to 104°F (0 to 40°C)
- Storage temperature: -13 to 158°F (-25 to 70°C)
- Humidity: 5 to 95% non-condensing

Powering on

To power on the FortiGate-100 unit:

- 1 Connect the AC adapter to the power connection at the back of the FortiGate-100 unit.
- 2 Connect the AC adapter to the power cable.
- 3 Connect the power cable to a power outlet.

The FortiGate-100 unit starts up. The Power and Status lights light. The Status light flashes while the FortiGate-100 unit is starting up and remains lit when the system is up and running.

Table 1: FortiGate-100 LED indicators

LED	State	Description
Power	Green	The FortiGate unit is powered on.
	Off	The FortiGate unit is powered off.
Status	Flashing green	The FortiGate unit is starting up.
	Green	The FortiGate unit is running normally.
	Off	The FortiGate unit is powered off.
Internal External DMZ (front)	Green	The correct cable is in use, and the connected equipment has power.
	Flashing green	Network activity at this interface.
	Off	No link established.
Internal External DMZ interfaces (back)	Green	The correct cable is in use, and the connected equipment has power.
	Flashing amber	Network activity at this interface.
	Off	No link established.

Connecting to the web-based manager

Use the following procedure to connect to the web-based manager for the first time. Configuration changes made with the web-based manager are effective immediately without the need to reset the firewall or interrupt service.

To connect to the web-based manager, you need:

- a computer with an ethernet connection,
- Internet Explorer version 4.0 or higher,
- a crossover cable or an ethernet hub and two ethernet cables.



Note: You can use the web-based manager with recent versions of most popular web browsers. The web-based manager is fully supported for Internet Explorer version 4.0 or higher.

Connecting to the web-based manager

- 1 Set the IP address of the computer with an ethernet connection to the static IP address 192.168.1.2 and a netmask of 255.255.255.0.
- 2 Using the crossover cable or the ethernet hub and cables, connect the Internal interface of the FortiGate unit to the computer ethernet connection.
- 3 Start Internet Explorer and browse to the address <https://192.168.1.99> (remember to include the “s” in https://).

The FortiGate login is displayed.

- 4 Type admin in the Name field and select Login.

The Register Now window is displayed. Use the information on this window to register your FortiGate unit so that Fortinet can contact you for firmware updates. You must also register to receive updates to the FortiGate virus and attack definitions.

Figure 3: FortiGate login

The screenshot shows the FortiGate web-based manager login interface. The header is teal with the Fortinet logo. A sidebar on the left lists various system components. The main area is light blue and displays the title 'FortiGate - 100'. Below the title is a login form with two input fields for 'Name' and 'Password', and a 'Login' button.

Connecting to the command line interface (CLI)

As an alternative to the web-based manager, you can install and configure the FortiGate unit using the CLI. Configuration changes made with the CLI are effective immediately without the need to reset the firewall or interrupt service.

To connect to the FortiGate CLI, you need:

- a computer with an available communications port,
- the null modem cable included in your FortiGate package,
- terminal emulation software such as HyperTerminal for Windows.



Note: The following procedure describes how to connect to the CLI using Windows HyperTerminal software. You can use any terminal emulation program.

To connect to the CLI:

- 1 Connect the null modem cable to the communications port of your computer and to the FortiGate Console port.
- 2 Make sure that the FortiGate unit is powered on.
- 3 Start HyperTerminal, enter a name for the connection, and select OK.
- 4 Configure HyperTerminal to connect directly to the communications port on the computer to which you have connected the null modem cable and select OK.
- 5 Select the following port settings and select OK.

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

- 6 Press Enter to connect to the FortiGate CLI.

The following prompt appears:

FortiGate-100 login:

- 7 Type admin and press Enter twice.

The following prompt appears:

Type ? for a list of commands.

For information on how to use the CLI, see the *FortiGate CLI Reference Guide*.

Factory default FortiGate configuration settings

The FortiGate unit is shipped with a factory default configuration. This default configuration allows you to connect to and use the FortiGate web-based manager to configure the FortiGate unit onto your network. To configure the FortiGate unit onto your network you add an administrator password, change network interface IP addresses, add DNS server IP addresses, and configuring routing if required.

If you are planning on operating the FortiGate unit in Transparent mode, you can switch to transparent mode from the factory default configuration and then configure the FortiGate unit onto your network in Transparent mode.

Once the network configuration is complete, you can perform additional configuration tasks such as setting system time, configuring virus and attack definition updates, and registering the FortiGate unit.

The factory default firewall configuration includes a single network address translation (NAT) policy that allows users on your internal network to connect to the external network, and stops users on the external network from connecting to the internal network. You can add more policies to provide more control of the network traffic passing through the FortiGate unit.

The factory default content profiles can be used to quickly apply different levels of antivirus protection, web content filtering, and email filtering to the network traffic controlled by firewall policies.

- [Factory default NAT/Route mode network configuration](#)
- [Factory default Transparent mode network configuration](#)
- [Factory default firewall configuration](#)
- [Factory default content profiles](#)

Factory default NAT/Route mode network configuration

When the FortiGate unit is first powered on, it is running in NAT/Route mode and has the basic network configuration listed in [Table 2](#). This configuration allows you to connect to the FortiGate unit web-based manager and establish the configuration required to connect the FortiGate unit to your network. In [Table 2](#) HTTPS management access means you can connect to the web-based manager using this interface. Ping management access means this interface responds to ping requests.

Table 2: Factory default NAT/Route mode network configuration

Administrator account		User name:	admin
		Password:	(none)
Internal interface		IP:	192.168.1.99
		Netmask:	255.255.255.0
		Management Access:	HTTPS, Ping
External interface	Manual:	IP:	192.168.100.99
		Netmask:	255.255.255.0
		Default Gateway:	192.168.100.1
		Primary DNS Server:	207.194.200.1
		Secondary DNS Server:	207.194.200.129
		Management Access:	Ping
DMZ interface		IP:	10.10.10.1
		Netmask:	255.255.255.0
		Management Access:	HTTPS, Ping

Factory default Transparent mode network configuration

If you switch the FortiGate unit to Transparent mode, it has the default network configuration listed in [Table 3](#).

Table 3: Factory default Transparent mode network configuration

Administrator account	User name:	admin
	Password:	(none)
Management IP	IP:	10.10.10.1
	Netmask:	255.255.255.0
DNS	Primary DNS Server:	207.194.200.1
	Secondary DNS Server:	207.194.200.129
Management access	Internal	HTTPS, Ping
	External	Ping
	DMZ	HTTPS, Ping

Factory default firewall configuration

The factory default firewall configuration is the same in NAT/Route and Transparent mode.

Table 4: Factory default firewall configuration

Internal Address	Internal_All	IP: 0.0.0.0	Represents all of the IP addresses on the internal network.
		Mask: 0.0.0.0	
External Address	External_All	IP: 0.0.0.0	Represents all of the IP addresses on the external network.
		Mask: 0.0.0.0	
DMZ Address	DMZ_All	IP: 0.0.0.0	Represents all of the IP addresses on the DMZ network.
		Mask: 0.0.0.0	
Recurring Schedule	Always		The schedule is valid at all times. This means that the firewall policy is valid at all times.
Firewall Policy	Int->Ext		Firewall policy for connections from the internal network to the external network.
	Source	Internal_All	The policy source address. Internal_All means that the policy accepts connections from any internal IP address.
	Destination	External_All	The policy destination address. External_All means that the policy accepts connections with a destination address to any IP address on the external network.
	Schedule	Always	The policy schedule. Always means that the policy is valid at any time.
	Service	ANY	The policy service. ANY means that this policy processes connections for all services.
	Action	ACCEPT	The policy action. ACCEPT means that the policy allows connections.
	☒ NAT		NAT is selected for the NAT/Route mode default policy so that the policy applies network address translation to the traffic processed by the policy. NAT is not available for Transparent mode policies.

Table 4: Factory default firewall configuration (Continued)

	☐ Traffic Shaping	Traffic shaping is not selected. The policy does not apply traffic shaping to the traffic controlled by the policy. You can select this option to control the maximum or minimum amount of bandwidth available to traffic processed by the policy.
	☐ Authentication	Authentication is not selected. Users do not have to authenticate with the firewall before connecting to their destination address. You can configure user groups and select this option to require users to authenticate with the firewall before they can connect through the firewall.
	☐ Antivirus & Web Filter	Antivirus & Web Filter is not selected. This policy does not include a content profile that applies antivirus protection, web content filtering, or email filtering to content traffic processed by this policy. You can select this option and select a content profile to apply different levels of content protection to traffic processed by this policy.
	☐ Log Traffic	Log Traffic is not selected. This policy does not record messages to the traffic log for the traffic processed by this policy. You can configure FortiGate logging and select Log Traffic to record all connections through the firewall that are accepted by this policy.

Factory default content profiles

You can use content profiles to apply different protection settings for content traffic controlled by firewall policies. You can use content profiles for:

- Antivirus protection of HTTP, FTP, IMAP, POP3, and SMTP network traffic
- Web content filtering for HTTP network traffic
- Email filtering for IMAP and POP3 network traffic
- Oversized file and email blocking for HTTP, FTP, POP3, SMTP, and IMAP network traffic
- Passing fragmented emails in IMAP, POP3, and SMTP email traffic

Using content profiles you can build up protection configurations that can be easily applied to different types of Firewall policies. This allows you to customize different types and different levels of protection for different firewall policies.

For example, while traffic between internal and external addresses might need strict protection, traffic between trusted internal addresses might need moderate protection. You can configure policies for different traffic services to use the same or different content profiles.

Content profiles can be added to NAT/Route mode and Transparent mode policies.

Strict content profile

Use the strict content profile to apply maximum content protection to HTTP, FTP, IMAP, POP3, and SMTP content traffic. You would not use the strict content profile under normal circumstances, but it is available if you are having extreme problems with viruses and require maximum content screening protection.

Table 5: Strict content profile

Options	HTTP	FTP	IMAP	POP3	SMTP
Antivirus Scan	☒	☒	☒	☒	☒
File Block	☒	☒	☒	☒	☒
Web URL Block	☒				
Web Content Block	☒				
Web Script Filter	☒				
Web Exempt List	☒				
Email Block List			☒	☒	
Email Exempt List			☒	☒	
Email Content Block			☒	☒	
Oversized File/Email Block	block	block	block	block	block
Pass Fragmented Emails			☐	☐	☐

Scan content profile

Use the scan content profile to apply antivirus scanning to HTTP, FTP, IMAP, POP3, and SMTP content traffic.

Table 6: Scan content profile

Options	HTTP	FTP	IMAP	POP3	SMTP
Antivirus Scan	☒	☒	☒	☒	☒
File Block	☐	☐	☐	☐	☐
Web URL Block	☐				
Web Content Block	☐				
Web Script Filter	☐				
Web Exempt List	☐				
Email Block List			☐	☐	
Email Exempt List			☐	☐	
Email Content Block			☐	☐	
Oversized File/Email Block	pass	pass	pass	pass	pass
Pass Fragmented Emails			☐	☐	☐

Web content profile

Use the web content profile to apply antivirus scanning and Web content blocking to HTTP content traffic. You can add this content profile to firewall policies that control HTTP traffic.

Table 7: Web content profile

Options	HTTP	FTP	IMAP	POP3	SMTP
Antivirus Scan	☒	☐	☐	☐	☐
File Block	☐	☐	☐	☐	☐
Web URL Block	☒				
Web Content Block	☒				
Web Script Filter	☐				
Web Exempt List	☐				
Email Block List	☐		☐	☐	
Email Exempt List			☐	☐	
Email Content Block			☐	☐	
Oversized File/Email Block	pass	pass	pass	pass	pass
Pass Fragmented Emails			☐	☐	☐

Unfiltered content profile

Use the unfiltered content profile if you do not want to apply any content protection to content traffic. You can add this content profile to firewall policies for connections between highly trusted or highly secure networks where content does not need to be protected.

Table 8: Unfiltered content profile

Options	HTTP	FTP	IMAP	POP3	SMTP
Antivirus Scan	☐	☐	☐	☐	☐
File Block	☐	☐	☐	☐	☐
Web URL Block	☐				
Web Content Block	☐				
Web Script Filter	☐				
Web Exempt List	☒				
Email Block List	☐		☐	☐	
Email Exempt List			☒	☒	
Email Content Block			☐	☐	
Oversized File/Email Block	pass	pass	pass	pass	pass
Pass Fragmented Emails			☒	☒	☒

Planning your FortiGate configuration

Before beginning to configure the FortiGate unit, you need to plan how to integrate the unit into your network. Among other things, you have to decide whether or not the unit will be visible to the network, which firewall functions it will provide, and how it will control the traffic flowing between its interfaces.

Your configuration plan is dependent upon the operating mode that you select. The FortiGate unit can be configured in either of two modes: NAT/Route mode (the default) or Transparent mode.

NAT/Route mode

In NAT/Route mode, the unit is visible to the network. Like a router, all of its interfaces are on different subnets. The following interfaces are available in NAT/Route mode:

- External is the interface to the external network (usually the Internet).
- Internal is the interface to the internal network.
- DMZ is the interface to the DMZ network.

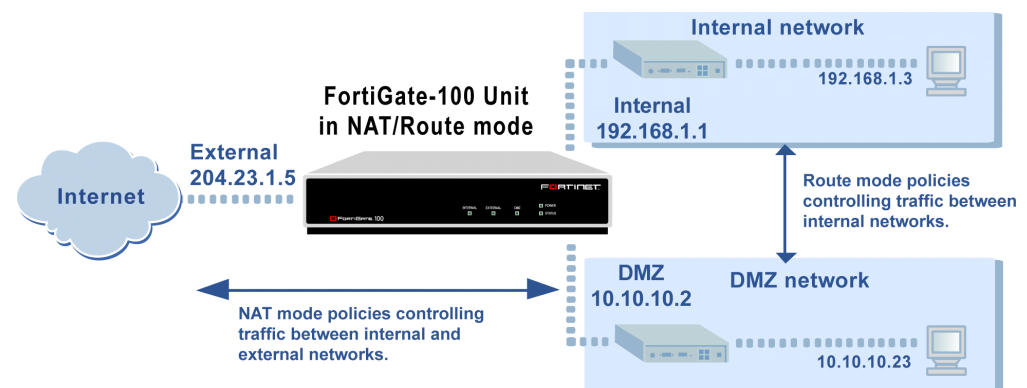
You can add security policies to control whether communications through the FortiGate unit operate in NAT mode or in route mode. Security policies control the flow of traffic based on each packet's source address, destination address and service. In NAT mode, the FortiGate performs network address translation before the packet is sent to the destination network. In route mode, no translation takes place.

By default, the FortiGate unit has a NAT mode security policy that allows users on the internal network to securely download content from the external network. No other traffic is possible until you have configured more security policies.

You would typically use NAT/Route mode when the FortiGate unit is used as a gateway between private and public networks. In this configuration, you would create NAT mode policies to control traffic flowing between the internal, private network and the external, public network (usually the Internet).

If you have multiple internal networks, such as a DMZ network in addition to the internal, private network, you could create route mode policies for traffic flowing between them.

Figure 4: Example NAT/Route mode network configuration



NAT/Route mode with multiple external network connections

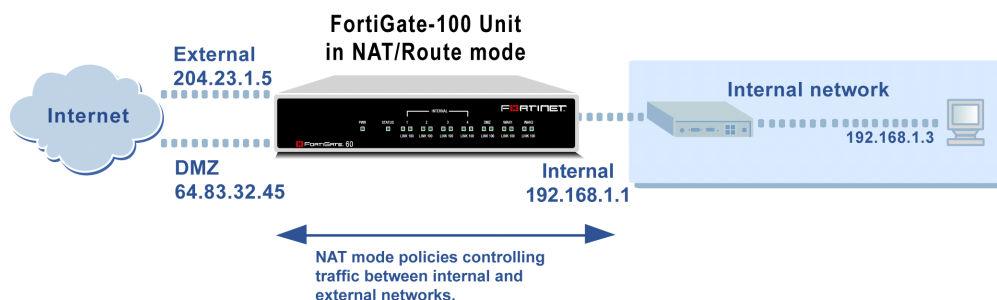
In NAT/Route mode, you can configure the FortiGate unit with multiple redundant connections to the external network (usually the Internet). For example, you could create the following configuration:

- External is the default interface to the external network (usually the Internet).
- DMZ is the redundant interface to the external network.
- Internal is the interface to the internal network.

You must configure routing to support redundant internet connections. Routing can be used to automatically re-direct connections from an interface if its connection to the external network fails.

Otherwise, security policy configuration is similar to a NAT/Route mode configuration with a single Internet connection. You would create NAT mode policies to control traffic flowing between the internal, private network and the external, public network (usually the Internet). If you have multiple internal networks, such as a DMZ network in addition to the internal, private network, you could create route mode policies for traffic flowing between them.

Figure 5: Example NAT/Route multiple internet connection configuration

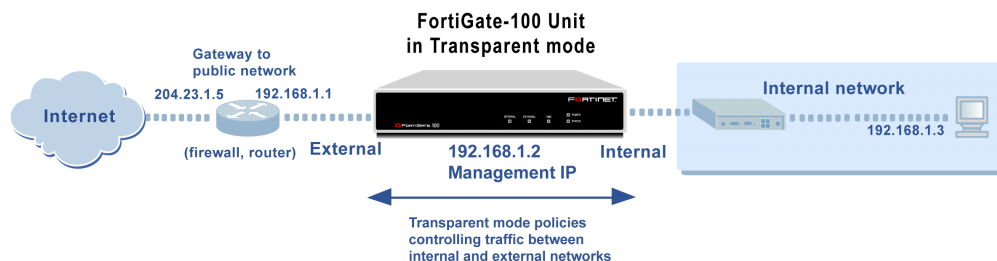


Transparent mode

In Transparent mode, the FortiGate unit is invisible to the network. Similar to a network bridge, all of FortiGate interfaces must be on the same subnet. You only have to configure a management IP address so that you can make configuration changes. The management IP address is also used for antivirus and attack definition updates.

You would typically use the FortiGate unit in Transparent mode on a private network behind an existing firewall or behind a router. The FortiGate unit performs firewalling as well as antivirus and content scanning but not VPN.

Figure 6: Example Transparent mode network configuration



You can connect up to three network segments to the FortiGate unit to control traffic between these network segments.

- External can connect to the external firewall or router.
- Internal can connect to the internal network.
- DMZ can connect to another network segment.

Configuration options

Once you have selected Transparent or NAT/Route mode operation, you can complete your configuration plan, and begin configuring the FortiGate unit.

You can use the web-based manager setup wizard or the command line interface (CLI) for the basic configuration of the FortiGate unit.

Setup Wizard

If you are configuring the FortiGate unit to operate in NAT/Route mode (the default), the Setup Wizard prompts you to add the administration password and the internal interface address. The Setup Wizard also prompts you to choose either a manual (static) or a dynamic (DHCP or PPPoE) address for the external interface. Using the wizard, you can also add DNS server IP addresses and a default route for the external interface.

In NAT/Route mode you can also configure the FortiGate DHCP server to supply IP addresses for the computers on your internal network. You can also configure the FortiGate to allow Internet access to your internal Web, FTP, or email servers.

If you are configuring the FortiGate unit to operate in Transparent mode, you can switch to Transparent mode from the web-based manager and then use the Setup Wizard to add the administration password, the management IP address and gateway, and the DNS server addresses.

CLI

If you are configuring the FortiGate unit to operate in NAT/Route mode, you can add the administration password and all interface addresses. You can also use the CLI to configure the external interface for either a manual (static) or a dynamic (DHCP or PPPoE) address. Using the CLI, you can also add DNS server IP addresses and a default route for the external interface.

In NAT/Route mode you can also configure the FortiGate DHCP server to supply IP addresses for the computers on your internal network.

If you are configuring the FortiGate unit to operate in Transparent mode, you can use the CLI to switch to Transparent mode. Then you can add the administration password, the management IP address and gateway, and the DNS server addresses.

FortiGate model maximum values matrix

Table 9: FortiGate maximum values matrix

	FortiGate model										
	50	60	100	200	300	400	500	1000	2000	3000	3600
Policy	200	500	1000	2000	5000	5000	20000	50000	50000	50000	50000
Address	500	500	500	500	3000	3000	6000	10000	10000	10000	10000
Address group	500	500	500	500	500	500	500	500	500	500	500
Service	500	500	500	500	500	500	500	500	500	500	500
Service group	500	500	500	500	500	500	500	500	500	500	500
Recurring schedule	256	256	256	256	256	256	256	256	256	256	256
Onetime schedule	256	256	256	256	256	256	256	256	256	256	256
User	20	500	1000	1000	1000	1000	1000	1000	1000	1000	1000
User group	100	100	100	100	100	100	100	100	100	100	100
Group members	300	300	300	300	300	300	300	300	300	300	300
Virtual IPs	500	500	500	500	500	500	500	500	500	500	500
IP/MAC binding	50	100	1000	1000	2000	2000	2000	5000	5000	5000	5000
Route	500	500	500	500	500	500	500	500	500	500	500
Policy route gateway	500	500	500	500	500	500	500	500	500	500	500
Admin user	500	500	500	500	500	500	500	500	500	500	500
IPsec Phase 1	20	50	80	200	1500	1500	3000	5000	5000	5000	5000
VPN concentrator	500	500	500	500	500	500	500	500	500	500	500
VLAN subinterface	N/A	N/A	N/A	N/A	N/A	1024*	1024*	2048*	2048*	8192*	8192*
Zone	N/A	N/A	N/A	N/A	N/A	100	100	200	200	300	500
IP pool	50	50	50	50	50	50	50	50	50	50	50
RADIUS server	6	6	6	6	6	6	6	6	6	6	6
File pattern	56	56	56	56	56	56	56	56	56	56	56
PPTP user	500	500	500	500	500	500	500	500	500	500	500
L2TP user	500	500	500	500	500	500	500	500	500	500	500
URL block	no limit	no limit	no limit	no limit	no limit	no limit	no limit	no limit	no limit	no limit	no limit
Content block	no limit	no limit	no limit	no limit	no limit	no limit	no limit	no limit	no limit	no limit	no limit
Exempt URL	no limit	no limit	no limit	no limit	no limit	no limit	no limit	no limit	no limit	no limit	no limit

Next steps

Now that your FortiGate unit is operating, you can proceed to configure it to connect to networks:

- If you are going to operate the FortiGate unit in NAT/Route mode, go to [“NAT/Route mode installation” on page 43](#).
- If you are going to operate the FortiGate unit in Transparent mode, go to [“Transparent mode installation” on page 57](#).

NAT/Route mode installation

This chapter describes how to install the FortiGate unit in NAT/Route mode. To install the FortiGate unit in Transparent mode, see [“Transparent mode installation” on page 57](#).

This chapter describes:

- [Preparing to configure NAT/Route mode](#)
- [Using the setup wizard](#)
- [Using the command line interface](#)
- [Connecting the FortiGate unit to your networks](#)
- [Configuring your networks](#)
- [Completing the configuration](#)
- [Configuration example: Multiple connections to the Internet](#)

Preparing to configure NAT/Route mode

Use [Table 10](#) to gather the information that you need to customize NAT/Route mode settings.

Table 10: NAT/Route mode settings

Administrator password:		
Internal interface	IP:	_____ . _____ . _____ . _____
	Netmask:	_____ . _____ . _____ . _____
External interface	IP:	_____ . _____ . _____ . _____
	Netmask:	_____ . _____ . _____ . _____
	Default Gateway:	_____ . _____ . _____ . _____
	Primary DNS Server:	_____ . _____ . _____ . _____
	Secondary DNS Server:	_____ . _____ . _____ . _____
Internal servers	Web Server:	_____ . _____ . _____ . _____
	SMTP Server:	_____ . _____ . _____ . _____
	POP3 Server:	_____ . _____ . _____ . _____
	IMAP Server:	_____ . _____ . _____ . _____
	FTP Server:	_____ . _____ . _____ . _____
If you provide access from the Internet to a web server, mail server, IMAP server, or FTP server installed on an internal network, add the IP addresses of the servers here.		

Advanced NAT/Route mode settings

Use [Table 11](#) to gather the information that you need to customize advanced FortiGate NAT/Route mode settings.

Table 11: Advanced FortiGate NAT/Route mode settings

External interface	DHCP:	If your Internet Service Provider (ISP) supplies you with an IP address using DHCP, no further information is required.	
	PPPoE:	User name:	
		Password:	
	If your ISP supplies you with an IP address using PPPoE, record your PPPoE user name and password.		
DHCP server	Starting IP:	____.____.____.____	
	Ending IP:	____.____.____.____	
	Netmask:	____.____.____.____	
	Default Route:	____.____.____.____	
	DNS IP:	____.____.____.____	
	The FortiGate unit contains a DHCP server that you can configure to automatically set the addresses of the computers on your internal network.		

DMZ interface

Use [Table 12](#) to record the IP address and netmask of the FortiGate DMZ interface if you are configuring it during installation.

Table 12: DMZ interface (Optional)

DMZ	IP:	____.____.____.____	Netmask:	____.____.____.____
------------	-----	---------------------	----------	---------------------

Using the setup wizard

From the web-based manager, you can use the setup wizard to create the initial configuration of your FortiGate unit. To connect to the web-based manager, see [“Connecting to the web-based manager” on page 30](#).

Starting the setup wizard

- 1 Select Easy Setup Wizard (the middle button in the upper-right corner of the web-based manager).
- 2 Use the information that you gathered in [Table 10 on page 43](#) to fill in the wizard fields. Select the Next button to step through the wizard pages.
- 3 Confirm your configuration settings and then select Finish and Close.



Note: If you use the setup wizard to configure internal server settings, the FortiGate unit adds port forwarding virtual IPs and firewall policies for each server. For each server located on your internal network the FortiGate unit adds an Ext->Int policy. For each server located on your DMZ network, the FortiGate unit adds an Ext->DMZ policy.

Reconnecting to the web-based manager

If you used the setup wizard to change the IP address of the internal interface, you must reconnect to the web-based manager using a new IP address. Browse to `https://` followed by the new IP address of the internal interface. Otherwise, you can reconnect to the web-based manager by browsing to `https://192.168.1.99`.

You have now completed the initial configuration of your FortiGate unit, and you can proceed to [“Connecting the FortiGate unit to your networks” on page 47](#).

Using the command line interface

As an alternative to using the setup wizard, you can configure the FortiGate unit using the command line interface (CLI). To connect to the CLI, see [“Connecting to the command line interface \(CLI\)” on page 31](#).

Configuring the FortiGate unit to operate in NAT/Route mode

Use the information that you gathered in [Table 10 on page 43](#) to complete the following procedures.

Configuring NAT/Route mode IP addresses

- 1 Log into the CLI if you are not already logged in.
- 2 Set the IP address and netmask of the internal interface to the internal IP address and netmask that you recorded in [Table 10 on page 43](#). Enter:
`set system interface internal mode static ip <IP address>
<netmask>`

Example

```
set system interface internal mode static ip 192.168.1.1  
255.255.255.0
```

- 3 Set the IP address and netmask of the external interface to the external IP address and netmask that you recorded in [Table 10 on page 43](#).
To set the manual IP address and netmask, enter:
set system interface external mode static ip <IP address>
<netmask>
Example
set system interface external mode static ip 204.23.1.5
255.255.255.0
To set the external interface to use DHCP, enter:
set system interface external mode dhcp connection enable
To set the external interface to use PPPoE, enter:
set system interface external mode pppoe username <user name>
password <password> connection enable
Example
set system interface external mode pppoe username
user@domain.com password mypass connection enable
- 4 Optionally set the IP address and netmask of the DMZ interface to the DMZ IP address and netmask that you recorded in [Table 12 on page 44](#). Enter:
set system interface dmz mode static ip <IP address> <netmask>
Example
set system interface dmz mode static ip 10.10.10.2
255.255.255.0
- 5 Confirm that the addresses are correct. Enter:
get system interface
The CLI lists the IP address, netmask and other settings for each of the FortiGate interfaces.
- 6 Set the primary DNS server IP addresses. Enter
set system dns primary <IP address>
Example
set system dns primary 293.44.75.21
- 7 Optionally, set the secondary DNS server IP addresses. Enter
set system dns secondary <IP address>
Example
set system dns secondary 293.44.75.22
- 8 Set the default route to the Default Gateway IP address (not required for DHCP and PPPoE).
set system route number <route_no> dst 0.0.0.0 0.0.0.0 gw1
<gateway_ip>
Example
set system route number 0 dst 0.0.0.0 0.0.0.0 gw1 204.23.1.2

Connecting the FortiGate unit to your networks

When you have completed the initial configuration, you can connect the FortiGate unit between your internal network and the Internet.

There are three 10/100Base-TX connectors on the FortiGate-100:

- Internal for connecting to your internal network
- External for connecting to the Internet
- DMZ for connecting to a DMZ network

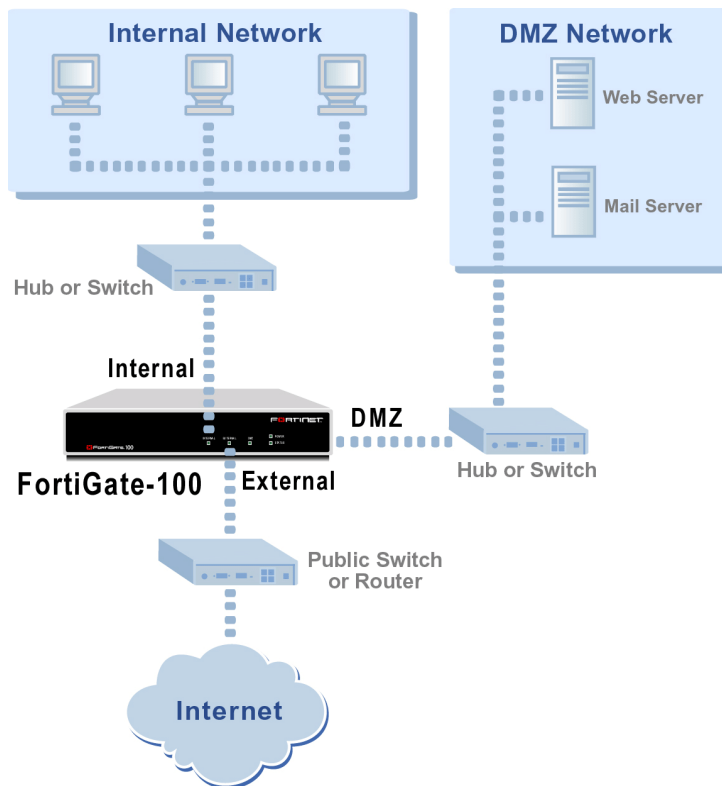


Note: You can also connect both the external and DMZ interfaces to different Internet connections to provide a redundant connection to the Internet. See [“Configuration example: Multiple connections to the Internet”](#) on page 49.

To connect the FortiGate unit:

- 1 Connect the Internal interface to the hub or switch connected to your internal network.
- 2 Connect the External interface to the Internet.
Connect to the public switch or router provided by your Internet Service Provider. If you are a DSL or cable subscriber, connect the External interface to the internal or LAN connection of your DSL or cable modem.
- 3 Optionally connect the DMZ interface to your DMZ network.
You can use a DMZ network to provide access from the Internet to a web server or other server without installing the servers on your internal network.

Figure 7: FortiGate-100 NAT/Route mode connections



Configuring your networks

If you are running the FortiGate unit in NAT/Route mode, your networks must be configured to route all Internet traffic to the IP address of the FortiGate interface to which they are connected. For your internal network, change the default gateway address of all computers and routers connected directly to your internal network to the IP address of the FortiGate internal interface. For your DMZ network, change the default gateway address of all computers and routers connected directly to your DMZ network to the IP address of the FortiGate DMZ interface. For your external network, route all packets to the FortiGate external interface.

If you are using the FortiGate unit as the DHCP server for your internal network, configure the computers on your internal network for DHCP.

Make sure that the connected FortiGate unit is functioning properly by connecting to the Internet from a computer on your internal network. You should be able to connect to any Internet address.

Completing the configuration

Use the information in this section to complete the initial configuration of the FortiGate unit.

Configuring the DMZ interface

If you are planning to configure a DMZ network, you might want to change the IP address of the DMZ interface. Use the following procedure to configure the DMZ interface using the web-based manager.

- 1 Log into the web-based manager.
- 2 Go to **System > Network > Interface**.
- 3 For the dmz interface, select Modify .
- 4 Change the IP address and Netmask as required.
- 5 Select Apply.

Setting the date and time

For effective scheduling and logging, the FortiGate system date and time should be accurate. You can either manually set the system date and time or you can configure the FortiGate unit to automatically keep its time correct by synchronizing with a Network Time Protocol (NTP) server.

To set the FortiGate system date and time, see [“Setting system date and time” on page 129](#).

- 1 Go to **Firewall > Policy > Int->Ext**.

Enabling antivirus protection

To enable antivirus protection to protect users on your internal network from downloading a virus from the Internet:

- 1 Go to **Firewall > Policy > Int->Ext**.
- 2 Select Edit  to edit this policy.
- 3 Select Anti-Virus & Web filter to enable antivirus protection for this policy.
- 4 Select the Scan Content Profile.
- 5 Select OK to save your changes.

Registering your FortiGate

After purchasing and installing a new FortiGate unit, you can register the unit by going to System > Update > Support, or using a web browser to connect to <http://support.fortinet.com> and selecting Product Registration.

Registration consists of entering your contact information and the serial numbers of the FortiGate units you or your organization have purchased. Registration is quick and easy. You can register multiple FortiGate units in a single session without re-entering your contact information.

For more information about registration, see [“Registering FortiGate units” on page 101](#).

Configuring virus and attack definition updates

You can go to System > Update to configure the FortiGate unit to automatically check to see if new versions of the virus definitions and attack definitions are available. If it finds new versions, the FortiGate unit automatically downloads and installs the updated definitions.

The FortiGate unit uses HTTPS on port 8890 to check for updates. The FortiGate external interface must have a path to the FortiResponse Distribution Network (FDN) using port 8890.

To configure automatic virus and attack updates, see [“Updating antivirus and attack definitions” on page 91](#).

Configuration example: Multiple connections to the Internet

This section describes some basic routing and firewall policy configuration examples for a FortiGate unit with multiple connections to the Internet (see [Figure 8](#)). In this topology, the organization operating the FortiGate unit uses two Internet service providers to connect to the Internet. The FortiGate unit is connected to the Internet using the external and DMZ interfaces. The external interface connects to gateway 1, operated by ISP1 and the DMZ interface connects to gateway 2, operated by ISP2.

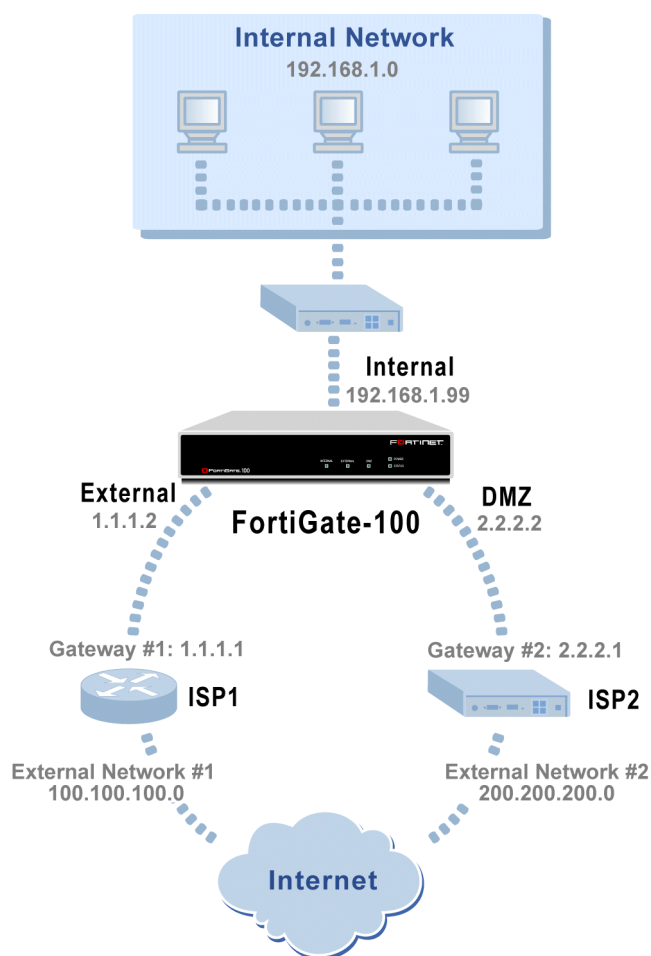
By adding ping servers to interfaces, and by configuring routing you can control how traffic uses each Internet connection. With this routing configuration in place you can proceed to create firewall policies to support multiple internet connections.

This section provides some examples of routing and firewall configurations to configure the FortiGate unit for multiple internet connections. To use the information in this section you should be familiar with FortiGate routing (see [“Configuring routing” on page 115](#)) and FortiGate firewall configuration (see [“Firewall configuration” on page 141](#)).

The examples below show how to configure destination-based routing and policy routing to control different traffic patterns.

- [Configuring Ping servers](#)
- [Destination based routing examples](#)
- [Policy routing examples](#)
- [Firewall policy example](#)

Figure 8: Example multiple Internet connection configuration



Configuring Ping servers

Use the following procedure to make Gateway 1 the ping server for the external interface and Gateway 2 the ping server for the DMZ interface.

- 1 Go to **System > Network > Interface**.
- 2 For the external interface, select Modify .
 - Ping Server: 1.1.1.1
 - Select Enable Ping Server
 - Select OK
- 3 For the DMZ interface, select Modify .
 - Ping Server: 2.2.2.1
 - Select Enable Ping Server
 - Select OK

Using the CLI

- 1 Add a ping server to the WAN1 interface.
- 1 Add a ping server to the external interface.

```
set system interface external config detectserver 1.1.1.1
gwdetect enable
```
- 2 Add a ping server to the DMZ interface.

```
set system interface dmz config detectserver 2.2.2.1 gwdetect
enable
```

Destination based routing examples

This section describes the following destination-based routing examples:

- [Primary and backup links to the Internet](#)
- [Load sharing](#)
- [Load sharing and primary and secondary connections](#)

Primary and backup links to the Internet

Use the following procedure to add a default destination-based route that directs all outgoing traffic to Gateway 1. If Gateway 1 fails, all connections are re-directed to Gateway 2. Gateway 1 is the primary link to the Internet and Gateway 2 is the backup link.

- 1 Go to **System > Network > Routing Table**.
- 2 Select New.
 - Destination IP: 0.0.0.0
 - Mask: 0.0.0.0
 - Gateway #1: 1.1.1.1
 - Gateway #2: 2.2.2.1
 - Device #1: external
 - Device #2: dmz
 - Select OK.

Using the CLI

- 1 Add the route to the routing table.

```
set system route number 0 dst 0.0.0.0 0.0.0.0 gw1 1.1.1.1
dev1 external gw2 2.2.2.1 dev2 dmz
```

Table 13: Route for primary and backup links

Destination IP ^a	Mask	Gateway #1	Device #1	Gateway #2	Device #2
0.0.0.0	0.0.0.0	1.1.1.1	external	2.2.2.1	dmz

Load sharing

You can also configure destination routing to direct traffic through both gateways at the same time. If users on your internal network connect to the networks of ISP1 and ISP2, you can add routes for each of these destinations. Each route can include a backup destination to the network of the other ISP.

Table 14: Load sharing routes

Destination IP ^a	Mask	Gateway #1	Device #1	Gateway #2	Device #2
100.100.100.0	255.255.255.0	1.1.1.1	external	2.2.2.1	dmz
200.200.200.0	255.255.255.0	2.2.2.1	dmz	1.1.1.1	external

The first route directs all traffic destined for the 100.100.100.0 network to gateway 1 with the IP address 1.1.1.1. If this router is down, traffic destined for the 100.100.100.0 network is re-directed to gateway 2 with the IP address 2.2.2.1.

Load sharing and primary and secondary connections

You can combine these routes into a more complete multiple internet connection configuration. In the topology shown in [Figure 8 on page 50](#), users on the Internal network would connect to the Internet to access web pages and other Internet resources. However, they may also connect to services, such as email, provided by their ISPs. You can combine the routes described in the previous examples to provide users with a primary and backup connection to the Internet, while at the same time routing traffic to each ISP network as required.

The routing described below allows a user on the internal network to connect to the Internet through gateway 1 and ISP1. At the same time, this user can also connect through the DMZ interface to gateway 2 to access a mail server maintained by ISP2.

Adding the routes using the web-based manager

- 1 Go to **System > Network > Routing Table**.
- 2 Select New to add the default route for primary and backup links to the Internet.
 - Destination IP: 0.0.0.0
 - Mask: 0.0.0.0
 - Gateway #1: 1.1.1.1
 - Gateway #2: 2.2.2.1
 - Device #1: external
 - Device #2: dmz
 - Select OK.

- 3 Select New to add a route for connections to the network of ISP1.
 - Destination IP: 100.100.100.0
 - Mask: 255.255.255.0
 - Gateway #1: 1.1.1.1
 - Gateway #2: 2.2.2.1
 - Device #1: external
 - Device #2: dmz
- 4 Select New to add a route for connections to the network of ISP2.
 - Destination IP: 200.200.200.0
 - Mask: 255.255.255.0
 - Gateway #1: 2.2.2.1
 - Gateway #2: 1.1.1.1
 - Device #1: external
 - Device #2: dmz
 - Select OK.
- 5 Change the order of the routes in the routing table to move the default route below the other two routes.
 - For the default route select Move to .
 - Type a number in the Move to field to move this route to the bottom of the list. If there are only 3 routes, type 3.
 - Select OK.

Adding the routes using the CLI

- 1 Add the route for connections to the network of ISP2.

```
set system route number 1 dst 100.100.100.0 255.255.255.0 gw1 1.1.1.1 dev1 external gw2 2.2.2.1 dev2 dmz
```
- 1 Add the route for connections to the network of ISP1.

```
set system route number 2 dst 200.200.200.0 255.255.255.0 gw1 2.2.2.1 dev1 dmz gw2 1.1.1.1 dev2 external
```
- 2 Add the default route for primary and backup links to the Internet.

```
set system route number 3 dst 0.0.0.0 0.0.0.0 gw1 1.1.1.1 dev1 external gw2 2.2.2.1 dev2 dmz
```

The routing table should have routes arranged as shown in [Table 15](#).

Table 15: Example combined routing table

Destination IP ^a	Mask	Gateway #1	Device #1	Gateway #2	Device #2
100.100.100.0	255.255.255.0	1.1.1.1	external	2.2.2.1	dmz
200.200.200.0	255.255.255.0	2.2.2.1	dmz	1.1.1.1	external
0.0.0.0	0.0.0.0	1.1.1.1	external	2.2.2.1	dmz

Policy routing examples

Policy routing can be added to increase the control you have over how packets are routed. Policy routing works on top of destination-based routing. This means you should configure destination-based routing first and then build policy routing on top to increase the control provided by destination-based routing.

For example, if you have used destination-based routing to configure routing for dual internet connections, you can use policy routing to apply more control to which traffic is sent to which destination route. This section describes the following policy routing examples, based on topology similar to that shown in [Figure 8 on page 50](#). Differences are noted in each example.

The policy routes described in these examples only work if you have already defined destination routes similar to those described in the previous section.

- [Routing traffic from internal subnets to different external networks](#)
- [Routing a service to an external network](#)

For more information about policy routing, see [“Policy routing” on page 118](#).

Routing traffic from internal subnets to different external networks

If the FortiGate unit provides internet access for multiple internal subnets, you can use policy routing to control the route that traffic from each network takes to the Internet. For example, if the internal network includes the subnets 192.168.10.0 and 192.168.20.0 you can enter the following policy routes:

- 1 Enter the following command to route traffic from the 192.168.10.0 subnet to the 100.100.100.0 external network:

```
set system route policy 1 src 192.168.10.0 255.255.255.0 dst 100.100.100.0 255.255.255.0 gw 1.1.1.1
```
- 2 Enter the following command to route traffic from the 192.168.20.0 subnet to the 200.200.200.0 external network:

```
set system route policy 2 src 192.168.20.0 255.255.255.0 dst 200.200.200.0 255.255.255.0 gw 2.2.2.1
```

Routing a service to an external network

You can use the following policy routes to direct all HTTP traffic (using port 80) to one external network and all other traffic to the other external network.

- 1 Enter the following command to route all HTTP traffic using port 80 to the next hop gateway with IP address 1.1.1.1.

```
set system route policy 1 src 0.0.0.0 0.0.0.0 dst 0.0.0.0 0.0.0.0 protocol 6 port 1 1000 gw 1.1.1.1
```
- 2 Enter the following command to route all other traffic to the next hop gateway with IP address 2.2.2.1.

```
Set system route policy 2 src 0.0.0.0 0.0.0.0 dst 0.0.0.0 0.0.0.0 gw 2.2.2.1
```

Firewall policy example

Firewall policies control how traffic flows through the FortiGate unit. Once routing for multiple internet connections has been configured you must create firewall policies to control which traffic is allowed through the FortiGate unit and the interfaces through which this traffic can connect.

For traffic originating on the Internal network to be able to connect to the Internet through both Internet connections, you must add redundant policies from the internal interface to each interface that connects to the Internet. Once these policies have been added, the routing configuration controls which internet connection is actually used.

Adding a redundant default policy

[Figure 8 on page 50](#) shows a FortiGate unit connected to the Internet using its internal and DMZ interfaces. The default policy allows all traffic from the internal network to connect to the Internet through the external interface. If you add a similar policy to the internal to DMZ policy list, this policy will allow all traffic from the internal network to connect to the Internet through the DMZ interface. With both of these policies added to the firewall configuration, the routing configuration will determine which Internet connection the traffic from the internal network actually uses. For more information about the default policy, see [“Default firewall configuration” on page 142](#).

To add a redundant default policy

- 1 Go to **Firewall > Policy > Int->DMZ**.
- 2 Select New.
- 3 Configure the policy to match the default policy.

Source	Internal_All
Destination	DMZ_All
Schedule	Always
Service	ANY
Action	Accept
NAT	Select NAT.

- 4 Select OK to save your changes.

Adding more firewall policies

In most cases your firewall configuration includes more than just the default policy. However, the basic premise of creating redundant policies applies even as the firewall configuration becomes more complex. To configure the FortiGate unit to use multiple Internet connections you must add duplicate policies for connections between the internal network and both interfaces connected to the Internet. As well, as you add redundant policies, you must arrange them in both policy lists in the same order.

Restricting access to a single Internet connection

In some cases you might want to limit some traffic to only being able to use one Internet connection. For example, in the topology shown in [Figure 8 on page 50](#) the organization might want its mail server to only be able to connect to the SMTP mail server of ISP1. To do this, you add a single Int->Ext firewall policy for SMTP connections. Because redundant policies have not been added, SMTP traffic from the Internet network is always connected to ISP1. If the connection to ISP1 fails the SMTP connection is not available.



Transparent mode installation

This chapter describes how to install your FortiGate unit in Transparent mode. If you want to install the FortiGate unit in NAT/Route mode, see [“NAT/Route mode installation” on page 43](#).

This chapter describes:

- [Preparing to configure Transparent mode](#)
- [Using the setup wizard](#)
- [Using the command line interface](#)
- [Connecting the FortiGate unit to your networks](#)
- [Completing the configuration](#)
- [Transparent mode configuration examples](#)

Preparing to configure Transparent mode

Use [Table 16](#) to gather the information that you need to customize Transparent mode settings.

Table 16: Transparent mode settings

Administrator Password:		
Management IP	IP:	_____ . _____ . _____ . _____
	Netmask:	_____ . _____ . _____ . _____
	Default Gateway:	_____ . _____ . _____ . _____
	The management IP address and netmask must be valid for the network from which you will manage the FortiGate unit. Add a default gateway if the FortiGate unit must connect to a router to reach the management computer.	
DNS Settings	Primary DNS Server:	_____ . _____ . _____ . _____
	Secondary DNS Server:	_____ . _____ . _____ . _____

Using the setup wizard

From the web-based manager, you can use the setup wizard to create the initial configuration of your FortiGate unit. To connect to the web-based manager, see [“Connecting to the web-based manager” on page 30](#).

Changing to Transparent mode

The first time that you connect to the FortiGate unit, it is configured to run in NAT/Route mode. To switch to Transparent mode using the web-based manager:

- 1 Go to **System > Status**.
- 2 Select Change to Transparent Mode.
- 3 Select Transparent in the Operation Mode list.
- 4 Select OK.

The FortiGate unit changes to Transparent mode.

To reconnect to the web-based manager, change the IP address of your management computer to 10.10.10.2. Connect to the internal or DMZ interface and browse to https:// followed by the Transparent mode management IP address. The default FortiGate Transparent mode management IP address is 10.10.10.1.

Starting the setup wizard

- 1 Select Easy Setup Wizard (the middle button in upper-right corner of the web-based manager).
- 2 Use the information that you gathered in [Table 16 on page 57](#) to fill in the wizard fields. Select the Next button to step through the wizard pages.
- 3 Confirm your configuration settings and then select Finish and Close.

Reconnecting to the web-based manager

If you changed the IP address of the management interface while you were using the setup wizard, you must reconnect to the web-based manager using the new IP address. Browse to https:// followed by the new IP address of the management interface. Otherwise, you can reconnect to the web-based manager by browsing to https://10.10.10.1. If you connect to the management interface through a router, make sure that you have added a default gateway for that router to the management IP default gateway field.

Using the command line interface

As an alternative to the setup wizard, you can configure the FortiGate unit using the command line interface (CLI). To connect to the CLI, see [“Connecting to the command line interface \(CLI\)” on page 31](#). Use the information that you gathered in [Table 16 on page 57](#) to complete the following procedures.

Changing to Transparent mode

- 1 Log into the CLI if you are not already logged in.
- 2 Switch to Transparent mode. Enter:
`set system opmode transparent`
After a few seconds, the login prompt appears.
- 3 Type `admin` and press Enter.
The following prompt appears:
Type `?` for a list of commands.
- 4 Confirm that the FortiGate unit has switched to Transparent mode. Enter:
`get system status`
The CLI displays the status of the FortiGate unit. The last line shows the current operation mode.
Operation mode: Transparent

Configuring the Transparent mode management IP address

- 1 Log into the CLI if you are not already logged in.
- 2 Set the management IP address and netmask to the IP address and netmask that you recorded in [Table 16 on page 57](#). Enter:
`set system management ip <IP address> <netmask>`
Example
`set system management ip 10.10.10.2 255.255.255.0`
- 3 Confirm that the address is correct. Enter:
`get system management`
The CLI lists the management IP address and netmask.

Configure the Transparent mode default gateway

- 1 Log into the CLI if you are not already logged in.
- 2 Set the default route to the default gateway that you recorded in [Table 16 on page 57](#). Enter:
`set system route number <number> gateway <IP address>`
Example
`set system route number 1 gw1 204.23.1.2`
You have now completed the initial configuration of the FortiGate unit.

Connecting the FortiGate unit to your networks

When you have completed the initial configuration, you can connect the FortiGate unit between your internal network and the Internet. You can also connect a network to the DMZ interface.

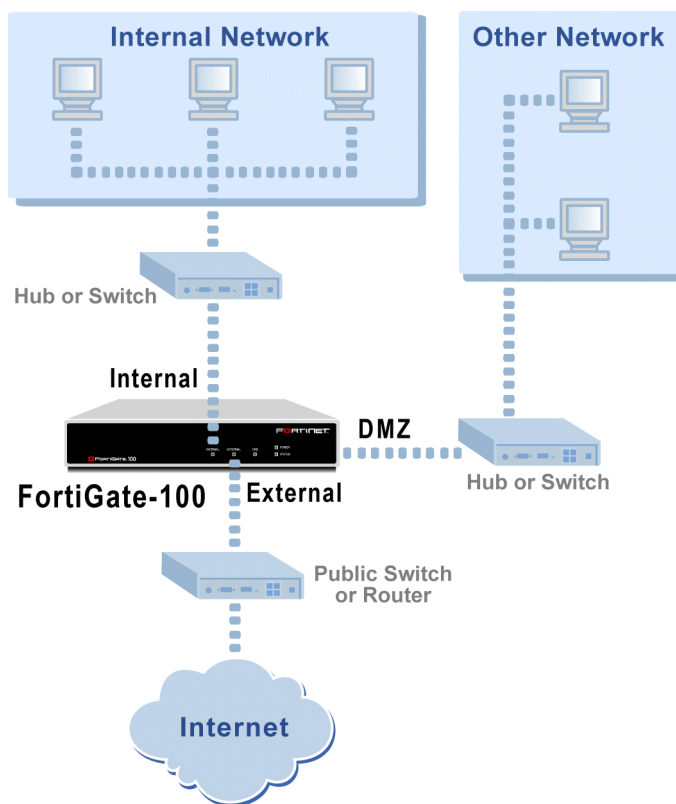
There are three 10/100Base-TX connectors on the FortiGate-100:

- Internal for connecting to your internal network
- External for connecting to the Internet
- DMZ for connecting to another network

To connect the FortiGate unit running in Transparent mode:

- 1 Connect the Internal interface to the hub or switch connected to your internal network.
- 2 Connect the External interface to the Internet.
Connect to the public switch or router provided by your Internet Service Provider.
- 3 Connect the DMZ interface to another network.

Figure 9: FortiGate-100 Transparent mode connections



In Transparent mode, the FortiGate unit does not change the layer 3 topology. This means that all of its interfaces are on the same IP subnet and that it appears to other devices as a bridge. Typically, the FortiGate unit would be deployed in Transparent mode when it is intended to provide antivirus and content scanning behind an existing firewall solution.

A FortiGate unit in Transparent mode can also perform firewalling. Even though it takes no part in the layer 3 topology, it can examine layer 3 header information and make decisions on whether to block or pass traffic.

Completing the configuration

Use the information in this section to complete the initial configuration of the FortiGate unit.

Setting the date and time

For effective scheduling and logging, the FortiGate system date and time should be accurate. You can either manually set the date and time or you can configure the FortiGate unit to automatically keep its date and time correct by synchronizing with a Network Time Protocol (NTP) server.

To set the FortiGate system date and time, see [“Setting system date and time” on page 129](#).

Enabling antivirus protection

To enable antivirus protection to protect users on your internal network from downloading a virus from the Internet:

- 1 Go to **Firewall > Policy > Int->Ext**.
- 2 Select Edit  to edit this policy.
- 3 Select Anti-Virus & Web filter to enable antivirus protection for this policy.
- 4 Select the Scan Content Profile.
- 5 Select OK to save your changes.

Registering your FortiGate

After purchasing and installing a new FortiGate unit, you can register the unit by going to System > Update > Support, or using a web browser to connect to <http://support.fortinet.com> and selecting Product Registration.

Registration consists of entering your contact information and the serial numbers of the FortiGate units you or your organization have purchased. Registration is quick and easy. You can register multiple FortiGate units in a single session without re-entering your contact information.

For more information about registration, see [“Registering FortiGate units” on page 101](#).

Configuring virus and attack definition updates

You can configure the FortiGate unit to automatically check to see if new versions of the virus definitions and attack definitions are available. If it finds new versions, the FortiGate unit automatically downloads and installs the updated definitions.

The FortiGate unit uses HTTPS on port 8890 to check for updates. The FortiGate external interface must have a path to the FortiResponse Distribution Network (FDN) using port 8890.

To configure automatic virus and attack updates, see [“Updating antivirus and attack definitions” on page 91](#).

Transparent mode configuration examples

A FortiGate unit operating in Transparent mode still requires a basic configuration to operate as a node on the IP network. As a minimum, the FortiGate unit must be configured with an IP address and subnet mask. These are used for management access and to allow the unit to receive antivirus and definitions updates. Also, the unit must have sufficient route information to reach:

- the management computer,
- The FortiResponse Distribution Network (FDN),
- a DNS server.

A route is required whenever the FortiGate unit connects to a router to reach a destination. If all of the destinations are located on the external network, you may be required to enter only a single default route. If, however, the network topology is more complex, you may be required to enter one or more static routes in addition to the default route.

This section describes:

- [Default routes and static routes](#)
- [Example default route to an external network](#)
- [Example static route to an external destination](#)
- [Example static route to an internal destination](#)

Default routes and static routes

To create a route to a destination, you need to define an IP prefix which consists of an IP network address and a corresponding netmask value. A default route matches any prefix and forwards traffic to the next hop router (otherwise known as the default gateway). A static route matches a more specific prefix and forwards traffic to the next hop router.

Default route example:

IP Prefix 0.0.0.0 (IP address)
0.0.0.0 (Netmask)

Next Hop 192.168.1.2

Static Route example:

IP Prefix 172.100.100.0 (IP address)
255.255.255.0 (Netmask)

Next Hop 192.168.1.2

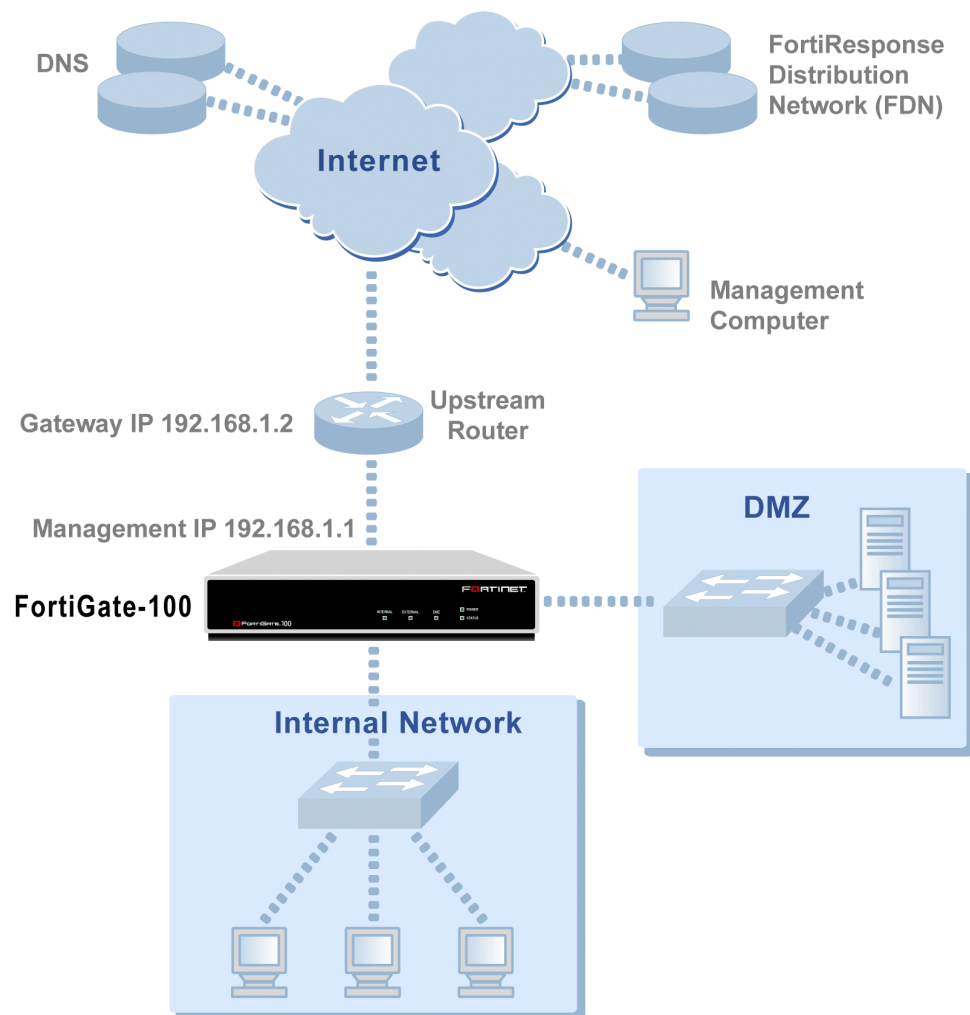


Note: When adding routes to the FortiGate unit, add the default route last so that it appears on the bottom of the route list. This ensures that the unit will attempt to match more specific routes before selecting the default route.

Example default route to an external network

Figure 10 shows a FortiGate unit where all destinations, including the management computer, are located on the external network. To reach these destinations, the FortiGate unit must connect to the “upstream” router leading to the external network. To facilitate this connection, you must enter a single default route that points to the upstream router as the next hop/default gateway.

Figure 10: Default route to an external network



General configuration steps

- 1 Set the FortiGate unit to operate in Transparent mode.
- 2 Configure the Management IP address and Netmask of the FortiGate unit.

- 3 Configure the default route to the external network.

Web-based manager example configuration steps

To configure basic Transparent mode settings and a default route using the web-based manager:

- 1 Go to **System > Status**.
 - Select Change to Transparent Mode.
 - Select Transparent in the Operation Mode list.
 - Select OK.
The FortiGate unit changes to Transparent mode.
- 2 Go to **System > Network > Management**.
 - Change the Management IP and Netmask:
IP: 192.168.1.1
Mask: 255.255.255.0
 - Select Apply.
- 3 Go to **System > Network > Routing**.
 - Select New to add the default route to the external network.
Destination IP: 0.0.0.0
Mask: 0.0.0.0
Gateway: 192.168.1.2
 - Select OK.

CLI configuration steps

To configure the Fortinet basic settings and a default route using the CLI:

- 1 Change the system to operate in Transparent Mode.
`set system opmode transparent`
- 2 Add the Management IP address and Netmask.
`set system management ip 192.168.1.1 255.255.255.0`
- 3 Add the default route to the external network.
`set system route number 1 gw1 192.168.1.2`

Example static route to an external destination

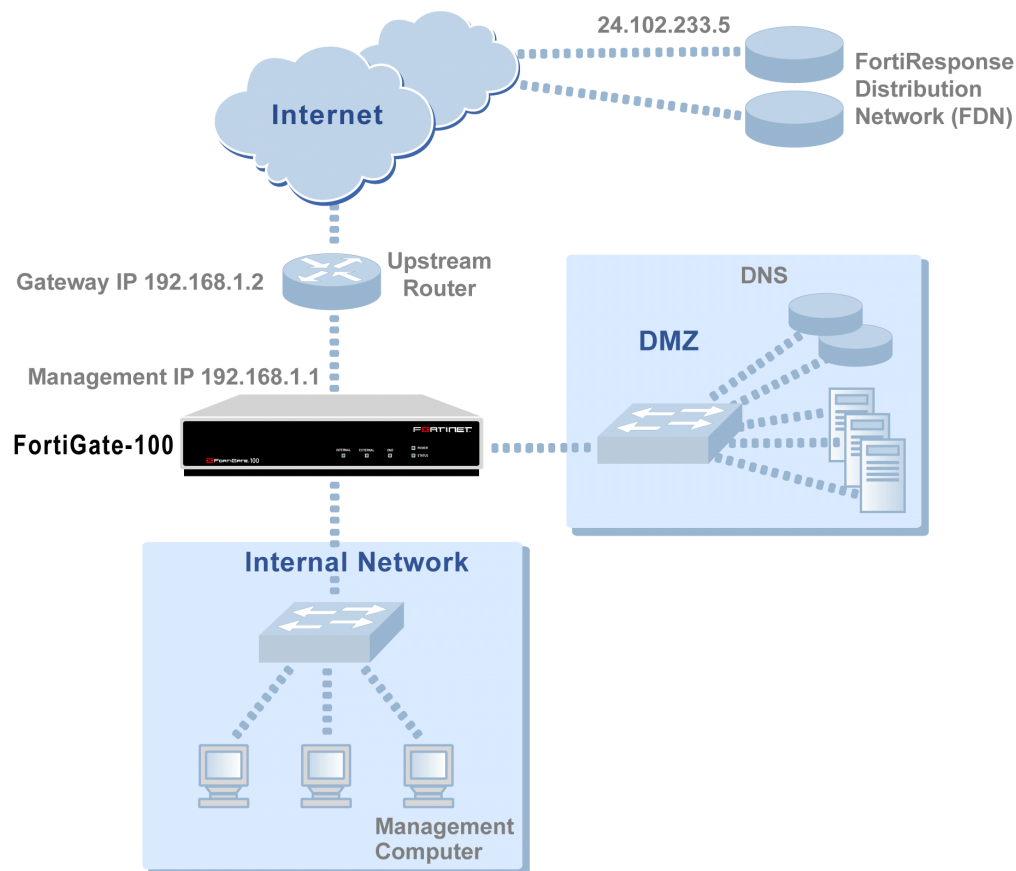
Figure 11 shows a FortiGate unit that requires routes to the FDN located on the external network. The Fortigate unit does not require routes to the DNS servers or management computer because they are located on the internal network.

To connect to the FDN, you would typically enter a single default route to the external network. However, to provide an extra degree of security, you could enter static routes to a specific FortiResponse server in addition to a default route to the external network. If the static route becomes unavailable (perhaps because the IP address of the FortiResponse server changes) the FortiGate unit will still be able to receive antivirus and NIDS updates from the FDN using the default route.



Note: This is an example configuration only. To configure a static route, you require a destination IP address.

Figure 11: Static route to an external destination



General configuration steps

- 1 Set the FortiGate unit to operate in Transparent mode.
- 2 Configure the Management IP address and Netmask of the FortiGate unit.
- 3 Configure the static route to the FortiResponse server.
- 4 Configure the default route to the external network.

Web-based manager example configuration steps

To configure the basic FortiGate settings and a static route using the web-based manager:

- 1 Go to **System > Status**.
 - Select Change to Transparent Mode.
 - Select Transparent in the Operation Mode list.
 - Select OK.
The FortiGate unit changes to Transparent mode.
- 2 Go to **System > Network > Management**.
 - Change the Management IP and Netmask:
IP: 192.168.1.1
Mask: 255.255.255.0
 - Select Apply.
- 3 Go to **System > Network > Routing**.
 - Select New to add the static route to the FortiResponse server.
Destination IP: 24.102.233.5
Mask: 255.255.255.0
Gateway: 192.168.1.2
 - Select OK.
 - Select New to add the default route to the external network.
Destination IP: 0.0.0.0
Mask: 0.0.0.0
Gateway: 192.168.1.2
 - Select OK.

CLI configuration steps

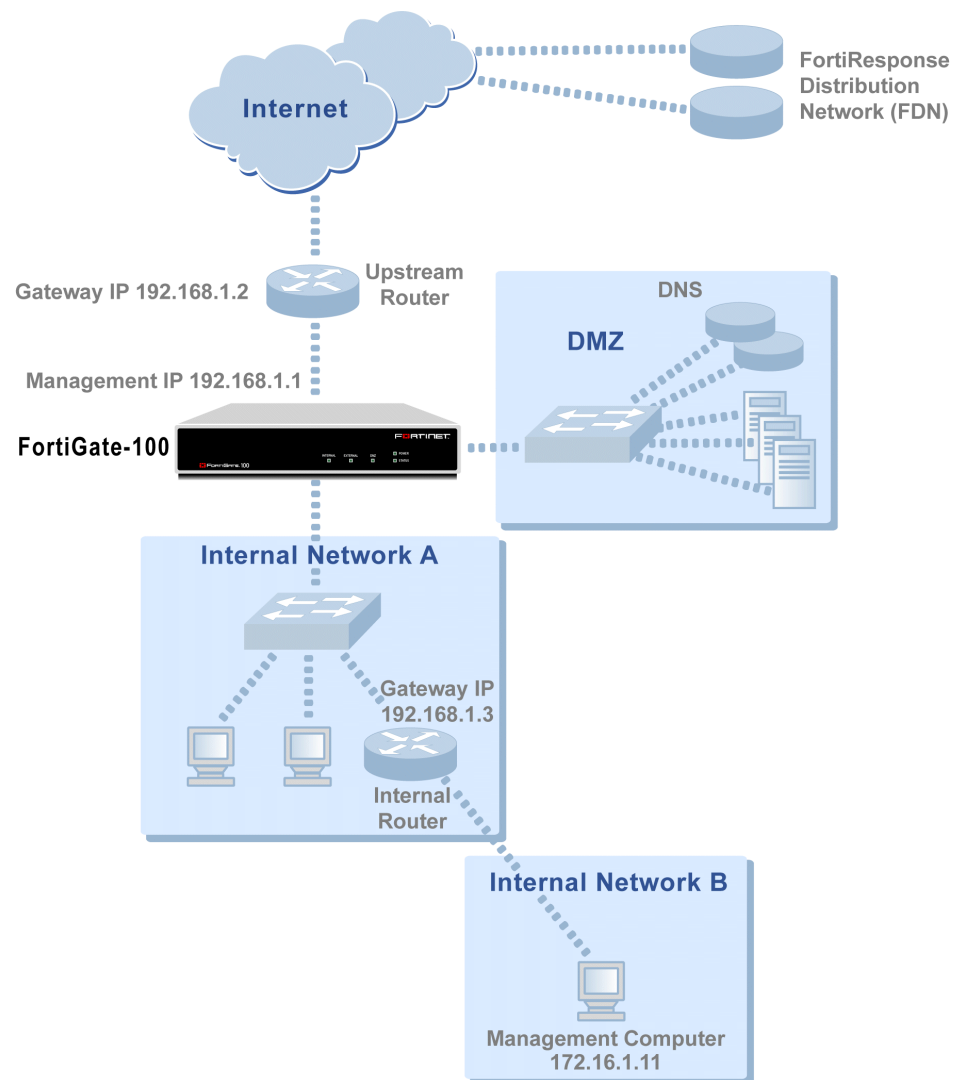
To configure the Fortinet basic settings and a static route using the CLI:

- 1 Set the system to operate in Transparent Mode.
`set system opmode transparent`
- 2 Add the Management IP address and Netmask.
`set system management ip 192.168.1.1 255.255.255.0`
- 3 Add the static route to the primary FortiResponse server.
`set system route number 1 dst 24.102.233.5 255.255.255.0 gw1 192.168.1.2`
- 4 Add the default route to the external network.
`set system route number 2 gw1 192.168.1.2`

Example static route to an internal destination

Figure 12 shows a FortiGate unit where the FDN is located on an external subnet and the management computer is located on a remote, internal subnet. To reach the FDN, you need to enter a single default route that points to the upstream router as the next hop/default gateway. To reach the management computer, you need to enter a single static route that leads directly to it. This route will point to the internal router as the next hop. (No route is required for the DNS servers because they are on the same layer 3 subnet as the FortiGate unit.)

Figure 12: Static route to an internal destination



General configuration steps

- 1 Set the unit to operate in Transparent mode.
- 2 Configure the Management IP address and Netmask of the FortiGate unit.
- 3 Configure the static route to the management computer on the internal network.
- 4 Configure the default route to the external network.

Web-based manager example configuration steps

To configure the FortiGate basic settings, a static route, and a default route using the web-based manager:

- 1 Go to **System > Status**.
 - Select Change to Transparent Mode.
 - Select Transparent in the Operation Mode list.
 - Select OK.
The FortiGate unit changes to Transparent mode.
- 2 Go to **System > Network > Management**.
 - Change the Management IP and Netmask:
IP: 192.168.1.1
Mask: 255.255.255.0
 - Select Apply.
- 3 Go to **System > Network > Routing**.
 - Select New to add the static route to the management computer.
Destination IP: 172.16.1.11
Mask: 255.255.255.0
Gateway: 192.168.1.3
 - Select OK.
 - Select New to add the default route to the external network.
Destination IP: 0.0.0.0
Mask: 0.0.0.0
Gateway: 192.168.1.2
 - Select OK.

CLI configuration steps

To configure the FortiGate basic settings, a static route, and a default route using the CLI:

- 1 Set the system to operate in Transparent Mode.
`set system opmode transparent`
- 2 Add the Management IP address and Netmask.
`set system management ip 192.168.1.1 255.255.255.0`
- 3 Add the static route to the management computer.
`set system route number 1 dst 172.16.1.11 255.255.255.0 gw1 192.168.1.3`
- 4 Add the default route to the external network.
`set system route number 2 gw1 192.168.1.2`



System status

You can connect to the web-based manager and go to **System > Status** to view the current status of your FortiGate unit. The status information that is displayed includes the current firmware version, the current virus and attack definitions, and the FortiGate unit serial number.

If you have logged into the web-based manager using the admin administrator account, you can use System Status to make any of the following changes to the FortiGate system settings:

- [Changing the FortiGate host name](#)
- [Changing the FortiGate firmware](#)
- [Manual virus definition updates](#)
- [Manual attack definition updates](#)
- [Backing up system settings](#)
- [Restoring system settings](#)
- [Restoring system settings to factory defaults](#)
- [Changing to Transparent mode](#)
- [Changing to NAT/Route mode](#)
- [Restarting the FortiGate unit](#)
- [Shutting down the FortiGate unit](#)

If you log into the web-based manager with any other administrator account, you can go to **System > Status** to view the system settings including:

- [Displaying the FortiGate serial number](#)
- [Displaying the FortiGate up time](#)

All administrative users can also go to **System > Status > Monitor** and view FortiGate system status. System status displays FortiGate health monitoring information including CPU and memory status, Session and network status.

- [System status](#)

All administrative users can also go to **System > Status > Session** and view the active communication sessions to and through the FortiGate unit.

- [Session list](#)

Changing the FortiGate host name

The FortiGate host name appears on the System > Status page and on the FortiGate CLI prompt. The host name is also used as the SNMP System Name (see [“Configuring SNMP” on page 134](#)).

The default host name is FortiGate-100.

To change the FortiGate host name:

- 1 Go to **System > Status**.
- 2 Select Edit Host Name .
- 3 Enter a new host name.
- 4 Select OK.

The new host name appears on the System Status page and is added to the SNMP System Name.

Changing the FortiGate firmware

After you download a FortiGate firmware image from Fortinet, you can use the procedures in [Table 1](#) to install the firmware image on your FortiGate unit.

Table 1: Firmware upgrade procedures

Procedure	Description
Upgrade to a new firmware version	Commonly-used web-based manager and CLI procedures to upgrade to a new FortiOS firmware version or to a more recent build of the same firmware version.
Revert to a previous firmware version	Use the web-based manager or CLI procedure to revert to a previous firmware version. This procedure reverts your FortiGate unit to its factory default configuration.
Install a firmware image from a system reboot using the CLI	Use this procedure to install a new firmware version or revert to a previous firmware version. You must run this procedure by connecting to the CLI using the FortiGate console port and a null-modem cable. This procedure reverts your FortiGate unit to its factory default configuration.
Test a new firmware image before installing it	Use this procedure to test a new firmware image before installing it. You must run this procedure by connecting to the CLI using the FortiGate console port and a null-modem cable. This procedure temporarily installs a new firmware image using your current configuration. You can test the firmware image before installing it permanently. If the firmware image works correctly you can use one of the other procedures listed in this table to install it permanently.
Installing and using a backup firmware image	If your FortiGate unit is running BIOS version v3.x, you can install a backup firmware image. Once the backup firmware image is installed you can switch to this backup image when required.

Upgrade to a new firmware version

Use the following procedures to upgrade your FortiGate to a newer firmware version.

Upgrading the firmware using the web-based manager



Note: Installing firmware replaces your current antivirus and attack definitions with the definitions included with the firmware release that you are installing. When you have installed new firmware, use the procedure [“Manually updating antivirus and attack definitions” on page 95](#) to make sure that antivirus and attack definitions are up-to-date.

- 1 Copy the firmware image file to your management computer.
- 2 Login to the FortiGate web-based manager as the admin administrative user.
- 3 Go to **System > Status**.
- 4 Select Firmware Upgrade .
- 5 Enter the path and filename of the firmware image file, or select Browse and locate the file.
- 6 Select OK.
The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiGate login. This process takes a few minutes.
- 7 Login to the web-based manager.
- 8 Go to **System > Status** and check the Firmware Version to confirm that the firmware upgrade has been installed successfully.
- 9 Use the procedure [“Manually updating antivirus and attack definitions” on page 95](#) to update antivirus and attack definitions.

Upgrading the firmware using the CLI

To use the following procedure you must have a TFTP server that you can connect to from the FortiGate unit.



Note: Installing firmware replaces your current antivirus and attack definitions with the definitions included with the firmware release that you are installing. When you have installed new firmware, use the procedure [“Manually updating antivirus and attack definitions” on page 95](#) to make sure that antivirus and attack definitions are up-to-date. You can also use the CLI command `execute updatecenter updatenow` to update the antivirus and attack definitions.

- 1 Make sure that the TFTP server is running.
- 2 Copy the new firmware image file to the root directory of the TFTP server.
- 3 Log into the CLI as the admin administrative user.
- 4 Make sure the FortiGate unit can connect to the TFTP server.
You can use the following command to ping the computer running the TFTP server. For example, if the TFTP server's IP address is 192.168.1.168:
`execute ping 192.168.1.168`

- 5 Enter the following command to copy the firmware image from the TFTP server to the FortiGate:

```
execute restore image <name_str> <tftp_ip>
```

Where <name_str> is the name of the firmware image file on the TFTP server and <tftp_ip> is the IP address of the TFTP server. For example, if the firmware image file name is FGT_300-v250-build045-FORTINET.out and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image FGT_300-v250-build045-FORTINET.out  
192.168.1.168
```

The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.

- 6 Reconnect to the CLI.
- 7 To confirm that the new firmware image has been loaded, enter:

```
get system status
```
- 8 Use the procedure [“Manually updating antivirus and attack definitions” on page 95](#) to update antivirus and attack definitions, or from the CLI, enter:

```
execute updatecenter updatenow
```
- 9 To confirm that the antivirus and attack definitions have been updated, enter the following command to display the antivirus engine, virus and attack definitions version, contract expiry, and last update attempt information.

```
get system objver
```

Revert to a previous firmware version

Use the following procedures to revert your FortiGate unit to a previous firmware version.

Reverting to a previous firmware version using the web-based manager

The following procedures return your FortiGate unit to its factory default configuration and delete NIDS user-defined signatures, web content lists, email filtering lists, and changes to replacement messages.

Before running this procedure you can:

- Backup the FortiGate unit configuration, use the procedure [“Backing up system settings” on page 83](#).
- Backup the NIDS user defined signatures, see the *FortiGate NIDS Guide*
- Backup web content and email filtering lists, see the *FortiGate Content Protection Guide*.

If you are reverting to a previous FortiOS version (for example, reverting from FortiOS v2.50 to FortiOS v2.36) you may not be able to restore your previous configuration from the backup configuration file.



Note: Installing firmware replaces your current antivirus and attack definitions with the definitions included with the firmware release that you are installing. When you have installed new firmware, use the procedure [“Manually updating antivirus and attack definitions” on page 95](#) to make sure that antivirus and attack definitions are up-to-date.

- 1 Copy the firmware image file to your management computer.
- 2 Login to the FortiGate web-based manager as the admin administrative user.
- 3 Go to **System > Status**.
- 4 Select Firmware Upgrade .
- 5 Enter the path and filename of the previous firmware image file, or select Browse and locate the file.
- 6 Select OK.

The FortiGate unit uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the FortiGate login. This process takes a few minutes.

- 7 Login to the web-based manager.

For information about logging into the web-based manager when the FortiGate unit is set to factory defaults, see [“Connecting to the web-based manager” on page 30](#).

- 8 Go to **System > Status** and check the Firmware Version to confirm that the firmware has been installed successfully.
- 9 Restore your configuration.

See [“Restoring system settings” on page 84](#) to restore your previous configuration.
- 10 Use the procedure [“Manually updating antivirus and attack definitions” on page 95](#) to update antivirus and attack definitions.

Reverting to a previous firmware version using the CLI

This procedure reverts your FortiGate unit to its factory default configuration and deletes NIDS user-defined signatures, web content lists, email filtering lists, and changes to replacement messages.

Before running this procedure you can:

- Backup the FortiGate unit configuration using the command `execute backup config`.
- Backup the NIDS user defined signatures using the command `execute backup nidsuserdefsig`
- Backup web content and email filtering lists, see the *FortiGate Content Protection Guide*.

If you are reverting to a previous FortiOS version (for example, reverting from FortiOS v2.50 to FortiOS v2.36) you may not be able to restore your previous configuration from the backup configuration file.



Note: Installing firmware replaces your current antivirus and attack definitions with the definitions included with the firmware release that you are installing. When you have installed new firmware, use the procedure [“Manually updating antivirus and attack definitions” on page 95](#) to make sure that antivirus and attack definitions are up-to-date. You can also use the CLI command `execute updatecenter updatenow` to update the antivirus and attack definitions.

To use the following procedure you must have a TFTP server that you can connect to from the FortiGate unit.

- 1 Make sure that the TFTP server is running.
- 2 Copy the new firmware image file to the root directory of the TFTP server.
- 3 Login to the FortiGate CLI as the admin administrative user.
- 4 Make sure the FortiGate unit can connect to the TFTP server.
You can use the following command to ping the computer running the TFTP server. For example, if the TFTP server's IP address is 192.168.1.168:
`execute ping 192.168.1.168`
- 5 Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:
`execute restore image <name_str> <tftp_ip>`

Where `<name_str>` is the name of the firmware image file on the TFTP server and `<tftp_ip>` is the IP address of the TFTP server. For example, if the firmware image file name is `FGT_300-v250-build045-FORTINET.out` and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image FGT_300-v250-build045-FORTINET.out
192.168.1.168
```

The FortiGate unit uploads the firmware image file. Once the file has been uploaded a message similar to the following is displayed:

```
Get image from tftp server OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
```

- 6 Type Y
- 7 The FortiGate unit reverts to the old firmware version, resets the configuration to factory defaults, and restarts. This process takes a few minutes.
- 8 Reconnect to the CLI.
For information about logging into the web-based manager when the FortiGate unit is set to factory defaults, see [“Connecting to the command line interface \(CLI\)” on page 31](#).
- 9 To confirm that the new firmware image has been loaded, enter:
`get system status`
- 10 Restore your previous configuration. Use the following command:
`execute restore config`
- 11 Use the procedure [“Manually updating antivirus and attack definitions” on page 95](#) to update antivirus and attack definitions, or from the CLI, enter:
`execute updatecenter updatenow`

- 12 To confirm that the antivirus and attack definitions have been updated, enter the following command to display the antivirus engine, virus and attack definitions version, contract expiry, and last update attempt information.
- ```
get system objver
```

## Install a firmware image from a system reboot using the CLI

This procedure installs a specified firmware image and resets the FortiGate unit to default settings. You can use this procedure to upgrade to a new firmware version, revert to an older firmware version, or to re-install the current firmware.



**Note:** There are a few variations on this procedure for different FortiGate BIOS versions. These variations are explained in the procedure steps that are affected. The version of the BIOS running on your FortiGate unit is displayed when you restart the FortiGate unit while accessing the CLI by connecting to the FortiGate console port using a null-modem cable.

To run this procedure you:

- access the CLI by connecting to the FortiGate console port using a null-modem cable,
- install a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

Before running this procedure you can:

- Backup the FortiGate unit configuration, use the procedure [“Backing up system settings” on page 83](#).
- Backup the NIDS user defined signatures, see the *FortiGate NIDS Guide*
- Backup web content and email filtering lists, see the *FortiGate Content Protection Guide*.

If you are reverting to a previous FortiOS version (for example, reverting from FortiOS v2.50 to FortiOS v2.36) you may not be able to restore your previous configuration from the backup configuration file.



**Note:** Installing firmware replaces your current antivirus and attack definitions with the definitions included with the firmware release that you are installing. When you have installed new firmware, use the procedure [“Manually updating antivirus and attack definitions” on page 95](#) to make sure that antivirus and attack definitions are up-to-date.

### To install firmware from a system reboot

- 1 Connect to the CLI using the null modem cable and FortiGate console port.
- 2 Make sure that the TFTP server is running.
- 3 Copy the new firmware image file to the root directory of your TFTP server.
- 4 Make sure that the internal interface is connected to the same network as the TFTP server.
- 5 To confirm that the FortiGate unit can connect to the TFTP server, use the following command to ping the computer running the TFTP server. For example, if the TFTP server's IP address is 192.168.1.168:  

```
execute ping 192.168.1.168
```

- 6 Enter the following command to restart the FortiGate unit:  
`execute reboot`  
As the FortiGate unit starts, a series of system startup messages are displayed.  
When one of the following messages appears:

- FortiGate unit running v2.x BIOS  
Press Any Key To Download Boot Image.  
...
- FortiGate unit running v3.x BIOS  
Press any key to enter configuration menu.....  
.....

- 7 Immediately press any key to interrupt the system startup.



**Note:** You only have 3 seconds to press any key. If you do not press any key soon enough, the FortiGate unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, one of the following messages appears:

- FortiGate unit running v2.x BIOS  
Enter TFTP Server Address [192.168.1.168]:  
Go to step 9.
- FortiGate unit running v3.x BIOS  
[G]: Get firmware image from TFTP server.  
[F]: Format boot device.  
[B]: Boot with backup firmware and set as default.  
[Q]: Quit menu and continue to boot with default firmware.  
[H]: Display this list of options.

Enter G, F, B, Q, or H:

- 8 Type G to get the new firmware image from the TFTP server.
- 9 Type the address of the TFTP server and press Enter.  
The following message appears:  
Enter Local Address [192.168.1.188]:
- 10 Type the address of the internal interface of the FortiGate unit and press Enter.



**Note:** The local IP address is only used to download the firmware image. After the firmware is installed the address of this interface is changed back to the default IP address for this interface.

The following message appears:  
Enter File Name [image.out]:

- 11 Enter the firmware image file name and press Enter.

The TFTP server uploads the firmware image file to the FortiGate unit and messages similar to the following appear.

- FortiGate unit running v2.x BIOS  
Do You Want To Save The Image? [Y/n]  
Type Y.
- FortiGate unit running v3.x BIOS  
Save as Default firmware/Run image without saving:[D/R]  
Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]  
Type D.

The FortiGate unit installs the new firmware image and restarts. The installation might take a few minutes to complete.

### Restoring your previous configuration

You can then restore your previous configuration. Begin by changing the interface addresses if required. You can do this from the CLI using the command:

```
set system interface
```

After changing the interface addresses, you can access the FortiGate unit from the web-based manager and restore your configuration.

To restore your FortiGate unit configuration, see [“Restoring system settings” on page 84](#). To restore NIDS user defined signatures, see the *FortiGate NIDS Guide*. To restore web content and email filtering lists, see the *FortiGate Content Protection Guide*.

If you are reverting to a previous firmware version (for example, reverting from FortiOS v2.50 to FortiOS v2.36) you may not be able to restore your previous configuration from the backup up configuration file.

- 12 Update the virus and attack definitions to the most recent version, see [“Manually updating antivirus and attack definitions” on page 95](#).

## Test a new firmware image before installing it

You can test a new firmware image by installing the firmware image from a system reboot and saving it to system memory. After completing this procedure the FortiGate unit operates using the new firmware image with the current configuration. This new firmware image is not permanently installed. The next time the FortiGate unit restarts it will be operating with the originally installed firmware image using the current configuration. If the new firmware image operates successfully, you can install it permanently using the procedure [“Upgrade to a new firmware version” on page 71](#).

To run this procedure you:

- access the CLI by connecting to the FortiGate console port using a null-modem cable,
- install a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

To test a new firmware image:

- 1 Connect to the CLI using a null modem cable and FortiGate console port.
- 2 Make sure the TFTP server is running.
- 3 Copy the new firmware image file to the root directory of the TFTP server.
- 4 Make sure that the internal interface is connected to the same network as the TFTP server.

You can use the following command to ping the computer running the TFTP server. For example, if the TFTP server's IP address is 192.168.1.168:

```
execute ping 192.168.1.168
```

- 5 Enter the following command to restart the FortiGate unit:  
`execute reboot`
- 6 As the FortiGate unit reboots, press any key to interrupt the system startup. As the FortiGate unit starts, a series of system startup messages are displayed. When one of the following messages appears:
  - FortiGate unit running v2.x BIOS  
Press Any Key To Download Boot Image.  
...
  - FortiGate unit running v3.x BIOS  
Press any key to enter configuration menu.....  
.....
- 7 Immediately press any key to interrupt the system startup.



**Note:** You only have 3 seconds to press any key. If you do not press any key soon enough, the FortiGate unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, one of the following messages appears:

- FortiGate unit running v2.x BIOS  
Enter TFTP Server Address [192.168.1.168]:  
Go to step 9.
- FortiGate unit running v3.x BIOS  
[G]: Get firmware image from TFTP server.  
[F]: Format boot device.  
[Q]: Quit menu and continue to boot with default firmware.  
[H]: Display this list of options.

Enter G, F, Q, or H:

- 8 Type G to get the new firmware image from the TFTP server.
- 9 Type the address of the TFTP server and press Enter.  
The following message appears:  
Enter Local Address [192.168.1.188]:
- 10 Type the address of the internal interface of the FortiGate unit and press Enter.



**Note:** The local IP address is only used to download the firmware image. After the firmware is installed the address of this interface is changed back to the default IP address for this interface.

The following message appears:

Enter File Name [image.out]:

- 11** Enter the firmware image file name and press Enter.

The TFTP server uploads the firmware image file to the FortiGate unit and messages similar to the following appear.

- FortiGate unit running v2.x BIOS  
Do You Want To Save The Image? [Y/n]  
Type N.
- FortiGate unit running v3.x BIOS  
Save as Default firmware/Run image without saving:[D/R]  
Type R.

The FortiGate image is installed to system memory and the FortiGate starts running the new firmware image but with its current configuration.

- 12** You can login to the CLI or the web-based manager using any administrative account.

- 13** To confirm that the new firmware image has been loaded, from the CLI enter:

```
get system status
```

You can test the new firmware image as required.

## Installing and using a backup firmware image

If your FortiGate unit is running BIOS version v3.x, you can install a backup firmware image. Once the backup firmware image is installed you can switch to this backup image when required.

This section describes:

- [Installing a backup firmware image](#)
- [Switching to the backup firmware image](#)
- [Switching back to the default firmware image](#)

### Installing a backup firmware image

To run this procedure you:

- access the CLI by connecting to the FortiGate console port using a null-modem cable,
- install a TFTP server that you can connect to from the FortiGate as described in the procedure [“Install a firmware image from a system reboot using the CLI” on page 75](#).

To install a backup firmware image:

- 1** Connect to the CLI using the null modem cable and FortiGate console port.
- 2** Make sure that the TFTP server is running.
- 3** Copy the new firmware image file to the root directory of your TFTP server.

- 4 To confirm that the FortiGate unit can connect to the TFTP server, use the following command to ping the computer running the TFTP server. For example, if the TFTP server's IP address is 192.168.1.168:

```
execute ping 192.168.1.168
```

- 5 Enter the following command to restart the FortiGate unit:

```
execute reboot
```

As the FortiGate unit starts, a series of system startup messages are displayed.

When one of the following messages appears:

```
Press any key to enter configuration menu.....
```

```
.....
```

- 6 Immediately press any key to interrupt the system startup.



**Note:** You only have 3 seconds to press any key. If you do not press any key soon enough, the FortiGate unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, one of the following messages appears:

```
[G]: Get firmware image from TFTP server.
```

```
[F]: Format boot device.
```

```
[B]: Boot with backup firmware and set as default.
```

```
[Q]: Quit menu and continue to boot with default firmware.
```

```
[H]: Display this list of options.
```

Enter G, F, B, Q, or H:

- 7 Type G to get the new firmware image from the TFTP server.
- 8 Type the address of the TFTP server and press Enter.  
The following message appears:  
Enter Local Address [192.168.1.188]:
- 9 Type the address of the interface of the FortiGate unit that can connect to the TFTP server and press Enter.  
The following message appears:  
Enter File Name [image.out]:
- 10 Enter the firmware image file name and press Enter.  
The TFTP server uploads the firmware image file to the FortiGate unit and messages similar to the following appear.  
Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]
- 11 Type B.

The FortiGate unit saves the backup firmware image and restarts. When the FortiGate unit restarts it is running the previously installed firmware version.

## Switching to the backup firmware image

Use this procedure to switch your FortiGate unit to operating with a backup firmware image that you have previously installed. When you switch the FortiGate unit to the backup firmware image, the FortiGate unit operates using the configuration that was saved with that firmware image.

If you install a new backup image from a reboot the configuration saved with this firmware image is the factory default configuration. If you use the procedure [“Switching back to the default firmware image” on page 82](#) to switch to a backup firmware image that was previously running as the default firmware image, the configuration saved with this firmware image is restored.

- 1 Connect to the CLI using the null modem cable and FortiGate console port.
- 2 Enter the following command to restart the FortiGate unit:  
`execute reboot`

As the FortiGate unit starts, a series of system startup messages are displayed.

When one of the following messages appears:

Press any key to enter configuration menu.....

.....

- 3 Immediately press any key to interrupt the system startup.



**Note:** You only have 3 seconds to press any key. If you do not press any key soon enough, the FortiGate unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, one of the following messages appears:

[G]: Get firmware image from TFTP server.

[F]: Format boot device.

[B]: Boot with backup firmware and set as default.

[Q]: Quit menu and continue to boot with default firmware.

[H]: Display this list of options.

Enter G, F, B, Q, or H:

- 4 Type B to load the backup firmware image.

The FortiGate unit loads the backup firmware image and restarts. When the FortiGate unit restarts it is running the backup firmware version and the configuration is set to factory default.

## Switching back to the default firmware image

Use this procedure to switch your FortiGate unit to operating with the backup firmware image that had been running as the default firmware image. When you switch to this backup firmware image, the configuration saved with this firmware image is restored.

- 1 Connect to the CLI using the null modem cable and FortiGate console port.
- 2 Enter the following command to restart the FortiGate unit:  
`execute reboot`

As the FortiGate unit starts, a series of system startup messages are displayed.

When one of the following messages appears:

Press any key to enter configuration menu.....

.....

- 3 Immediately press any key to interrupt the system startup.



**Note:** You only have 3 seconds to press any key. If you do not press any key soon enough, the FortiGate unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, one of the following messages appears:

[G]: Get firmware image from TFTP server.

[F]: Format boot device.

[B]: Boot with backup firmware and set as default.

[Q]: Quit menu and continue to boot with default firmware.

[H]: Display this list of options.

Enter G, F, B, Q, or H:

- 4 Type B to load the backup firmware image.

The FortiGate unit loads the backup firmware image and restarts. When the FortiGate unit restarts it is running the backup firmware version with a restored configuration.

## Manual virus definition updates

The System > Status page of the FortiGate web-based manager displays the current installed versions of the FortiGate Antivirus Definitions. You can use the following procedure to update the antivirus definitions manually.



**Note:** To configure the FortiGate unit for automatic antivirus definitions updates, see [“Virus and attack definitions updates and registration” on page 91](#). You can also manually initiate an antivirus definitions update by going to **System > Update** and selecting Update Now.

- 1 Download the latest antivirus definitions update file from Fortinet and copy it to the computer that you use to connect to the web-based manager.
- 2 Start the web-based manager and go to **System > Status**.
- 3 To the right of the Antivirus Definitions Version, select Definitions Update .
- 4 Enter the path and filename for the antivirus definitions update file, or select Browse and locate the antivirus definitions update file.

- 5 Select OK to copy the antivirus definitions update file to the FortiGate unit.  
The FortiGate unit updates the antivirus definitions. This takes about 1 minute.
- 6 Go to **System > Status** to confirm that the Antivirus Definitions Version information has been updated.

## Manual attack definition updates

The System > Status page of the FortiGate web-based manager displays the current installed versions of the FortiGate Attack Definitions used by the Network Intrusion Detection System (NIDS). You can use the following procedure to update the attack definitions manually.



**Note:** To configure the FortiGate unit for automatic attack definitions updates, see [“Virus and attack definitions updates and registration” on page 91](#). You can also manually initiate an attack definitions update by going to **System > Update** and selecting Update Now.

- 1 Download the latest attack definitions update file from Fortinet and copy it to the computer that you use to connect to the web-based manager.
- 2 Start the web-based manager and go to **System > Status**.
- 3 To the right of the Attack Definitions Version, select Definitions Update .
- 4 Enter the path and filename for the attack definitions update file, or select Browse and locate the attack definitions update file.
- 5 Select OK to copy the attack definitions update file to the FortiGate unit.  
The FortiGate unit updates the attack definitions. This takes about 1 minute.
- 6 Go to **System > Status** to confirm that the Attack Definitions Version information has been updated.

## Displaying the FortiGate serial number

- 1 Go to **System > Status**.  
The serial number is displayed in the System Status page of the web-based manager. The serial number is specific to the FortiGate unit and does not change with firmware upgrades.

## Displaying the FortiGate up time

- 1 Go to **System > Status**.  
The FortiGate up time displays the time in days, hours, and minutes since the FortiGate unit was last started.

## Backing up system settings

You can back up system settings by downloading them to a text file on the management computer:

- 1 Go to **System > Status**.

- 2 Select System Settings Backup.
- 3 Select Backup System Settings.
- 4 Type a name and location for the file.  
The system settings file is backed up to the management computer.
- 5 Select Return to go back to the Status page.

## Restoring system settings

You can restore system settings by uploading a previously downloaded system settings text file:

- 1 Go to **System > Status**.
- 2 Select System Settings Restore.
- 3 Enter the path and filename of the system settings file, or select Browse and locate the file.
- 4 Select OK to restore the system settings file to the FortiGate unit.  
The FortiGate unit restarts, loading the new system settings.
- 5 Reconnect to the web-based manager and review your configuration to confirm that the uploaded system settings have taken effect.

## Restoring system settings to factory defaults

Use the following procedure to restore system settings to the values set at the factory. This procedure does not change the firmware version or the antivirus or attack definitions.



**Caution:** This procedure deletes all changes that you have made to the FortiGate configuration and reverts the system to its original configuration, including resetting interface addresses.

- 1 Go to **System > Status**.
- 2 Select Restore Factory Defaults.
- 3 Select OK to confirm.  
The FortiGate unit restarts with the configuration that it had when it was first powered on.
- 4 Reconnect to the web-based manager and review the system configuration to confirm that it has been reset to the default settings.  
To restore your system settings, see [“Restoring system settings” on page 84](#).

## Changing to Transparent mode

Use the following procedure to switch the FortiGate unit from NAT/Route mode to Transparent mode. When the FortiGate unit has changed to Transparent mode its configuration resets to Transparent mode factory defaults.

- 1 Go to **System > Status**.
- 2 Select Change to Transparent Mode.
- 3 Select Transparent in the operation mode list.
- 4 Select OK.  
The FortiGate unit changes operation mode.
- 5 To reconnect to the web-based manager, connect to the interface configured for Transparent mode management access and browse to https:// followed by the Transparent mode management IP address.  
By default in Transparent mode, you can connect to the internal or DMZ interface. The default Transparent mode management IP address is 10.10.10.1.

## Changing to NAT/Route mode

Use the following procedure to switch the FortiGate unit from Transparent mode to NAT/Route mode. When the FortiGate unit has changed to NAT/Route mode its configuration resets to NAT/Route mode factory defaults.

- 1 Go to **System > Status**.
- 2 Select Change to NAT Mode.
- 3 Select NAT/Route in the operation mode list.
- 4 Select OK.  
The FortiGate unit changes operation mode.
- 5 To reconnect to the web-based manager you must connect to the interface configured by default for management access.  
By default in NAT/Route mode, you can connect to the internal or DMZ interface. The default Transparent mode management IP address is 192.168.1.99.  
See [“Connecting to the web-based manager” on page 30](#) or [“Connecting to the command line interface \(CLI\)” on page 31](#).

## Restarting the FortiGate unit

- 1 Go to **System > Status**.
- 2 Select Restart.  
The FortiGate unit restarts.

## Shutting down the FortiGate unit

- 1 Go to **System > Status**.
- 2 Select Shutdown.  
The FortiGate unit shuts down and all traffic flow stops.  
The FortiGate unit can only be restarted after shutdown by turning the power off, then on.

## System status

You can use the system status monitor to display FortiGate system health information. The system health information includes memory usage, the number of active communication sessions, and the amount of network bandwidth currently in use. The web-based manager displays current statistics as well as statistics for the previous minute.

You can also view current virus and intrusion status. The web-based manager displays the current number of viruses and attacks as well as a graph of virus and attack levels over the previous 20 hours.

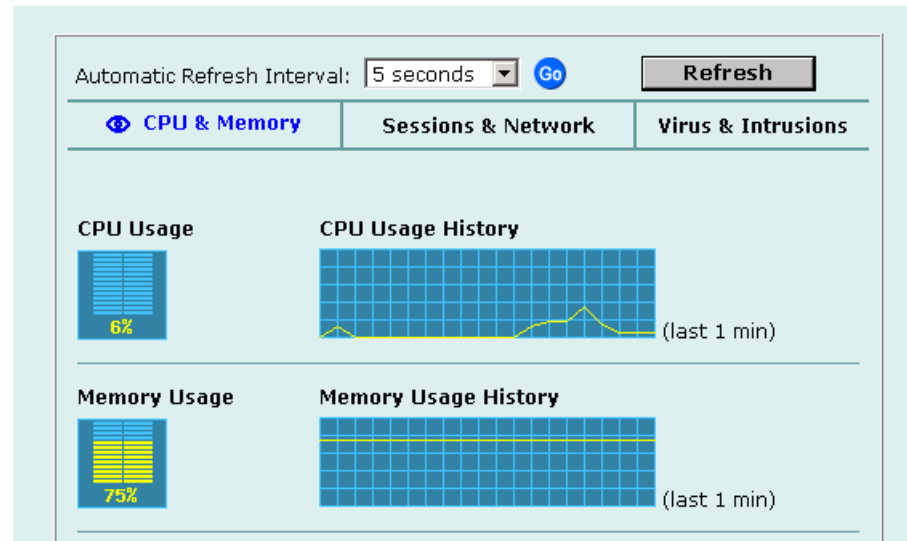
In each case you can set an automatic refresh interval that updates the display every 5 to 30 seconds. You can also refresh the display manually.

- [Viewing CPU and memory status](#)
- [Viewing sessions and network status](#)
- [Viewing virus and intrusions status](#)

### Viewing CPU and memory status

Current CPU and memory status indicates how close the FortiGate unit is to running at full capacity. The web-based manager displays CPU and memory usage for core processes only. CPU and memory use for management processes (for example, for HTTPS connections to the web-based manager) is excluded.

If CPU and memory use is low, the FortiGate unit is able to process much more network traffic than is currently running. If CPU and memory use is high, the FortiGate unit is performing near its full capacity. Placing additional demands on the system could lead to traffic processing delays.

**Figure 1: CPU and memory status monitor**

CPU and memory intensive processes such as encrypting and decrypting IPsec VPN traffic, virus scanning, and processing high levels of network traffic containing small packets will increase CPU and memory usage.

- 1 Go to **System > Status > Monitor**.

CPU & Memory status is displayed. The display includes bar graphs of current CPU and memory usage as well as line graphs of CPU and memory usage for the last minute.

- 2 Set the automatic refresh interval and select Go to control how often the web-based manager updates the display.

More frequent updates use system resources and increase network traffic. However, this only occurs when you are viewing the display using the web-based manager.

- 3 Select Refresh to manually update the information displayed.

## Viewing sessions and network status

Use the session and network status display to track how many network sessions the FortiGate unit is processing and to see what effect the number of sessions has on the available network bandwidth. Also, by comparing CPU and memory usage with session and network status you can see how much demand network traffic is placing on system resources.

Sessions displays the total number of sessions being processed by the FortiGate unit on all interfaces. Sessions also displays the sessions as a percentage of the maximum number of sessions that the FortiGate unit is designed to support.

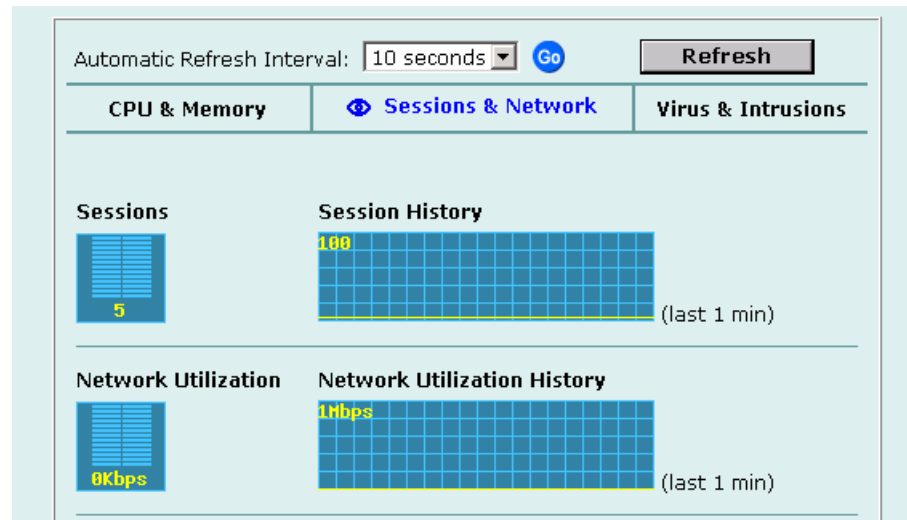
Network utilization displays the total network bandwidth being used through all FortiGate interfaces. Network utilization also displays network utilization as a percentage of the maximum network bandwidth that can be processed by the FortiGate unit.

- 1 Go to **System > Status > Monitor**.

**2** Select Sessions & Network.

Sessions and network status is displayed. The display includes bar graphs of the current number of sessions and current network utilization as well as line graphs of session and network utilization usage for the last minute. The line graph scales are shown in the upper left corner of the graph.

**Figure 2: Sessions and network status monitor**



**3** Set the automatic refresh interval and select Go to control how often the web-based manager updates the display.

More frequent updates use system resources and increase network traffic. However, this only occurs when you are viewing the display using the web-based manager.

**4** Select Refresh to manually update the information displayed.

## Viewing virus and intrusions status

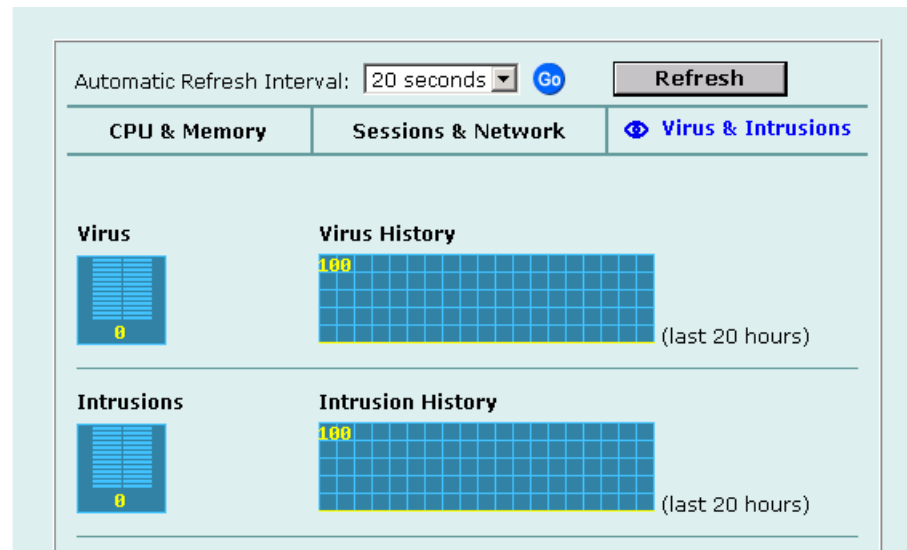
Use the virus and intrusions status display to track when viruses are found by the FortiGate antivirus system and to track when the NIDS detects a network-based attack.

**1** Go to **System > Status > Monitor**.

**2** Select Virus & Intrusions.

Virus and intrusions status is displayed. The display includes bar graphs of the number viruses and intrusions detected per hour as well as line graphs of the number of viruses and intrusions detected for the last 20 hours.

Figure 3: Sessions and network status monitor



- 3 Set the automatic refresh interval and select Go to control how often the web-based manager updates the display.  
More frequent updates use system resources and increase network traffic. However, this only occurs when you are viewing the display using the web-based manager. The line graph scales are shown on the upper right corner of the graph.
- 4 Select Refresh to manually update the information displayed.

## Session list

The session list displays information about the communications sessions currently being processed by the FortiGate unit. You can use the session list to view current sessions. FortiGate administrators with read and write permission, and the FortiGate admin user can also stop active communication sessions.

### Viewing the session list

- 1 Go to **System > Status > Session**.  
The web-based manager displays the total number of active sessions in the FortiGate unit session table and lists the top 16.
- 2 To page through the list of sessions, select Page Up  or Page Down .
- 3 Select Refresh  to update the session list.
- 4 If you have logged in as an administrative user with read and write privileges or as the admin user, you can select Clear  to stop any active session.

Each line of the session list displays the following information:

|                  |                                                                         |
|------------------|-------------------------------------------------------------------------|
| <b>Protocol</b>  | The service protocol of the connection, for example, udp, tcp, or icmp. |
| <b>From IP</b>   | The source IP address of the connection.                                |
| <b>From Port</b> | The source port of the connection.                                      |

**To IP** The destination IP address of the connection.  
**To Port** The destination port of the connection.  
**Expire** The time, in seconds, before the connection expires.  
**Clear** Stop an active communication session.

Figure 4: Example session list

| Total Number of Sessions: 659 |                 |           |               |         |               |                                                                                       |
|-------------------------------|-----------------|-----------|---------------|---------|---------------|---------------------------------------------------------------------------------------|
| Protocol                      | From IP         | From Port | To IP         | To Port | Expire (secs) | Clear                                                                                 |
| udp                           | 192.168.110.200 | 1242      | 206.191.0.210 | 53      | 76            |    |
| tcp                           | 192.168.110.121 | 4704      | 192.168.110.3 | 443     | 8             |    |
| tcp                           | 192.168.110.200 | 1250      | 65.39.139.188 | 110     | 42            |    |
| tcp                           | 192.168.110.121 | 4699      | 192.168.110.3 | 443     | 8             |    |
| tcp                           | 192.168.110.121 | 4691      | 192.168.110.3 | 443     | 56            |    |
| tcp                           | 192.168.110.121 | 4479      | 10.0.1.128    | 6969    | 72            |    |
| udp                           | 192.168.110.200 | 1246      | 209.87.239.20 | 53      | 86            |    |
| udp                           | 192.168.110.200 | 1246      | 209.87.239.21 | 53      | 89            |    |
| tcp                           | 192.168.110.121 | 4674      | 192.168.110.3 | 443     | 8             |    |
| tcp                           | 192.168.110.155 | 1107      | 65.39.139.188 | 143     | 3262          |    |
| tcp                           | 192.168.110.200 | 1248      | 65.39.139.188 | 110     | 30            |    |
| tcp                           | 192.168.110.123 | 2307      | 65.39.139.188 | 110     | 26            |    |
| tcp                           | 192.168.110.121 | 4701      | 192.168.110.3 | 443     | 8             |    |
| tcp                           | 192.168.110.154 | 1117      | 65.39.139.188 | 143     | 962           |   |
| tcp                           | 192.168.110.121 | 4361      | 10.0.1.128    | 6969    | 49            |  |
| tcp                           | 192.168.110.123 | 2308      | 65.39.139.188 | 110     | 85            |  |
| tcp                           | 192.168.110.121 | 4708      | 192.168.110.3 | 443     | 58            |  |

# Virus and attack definitions updates and registration

You can configure the FortiGate unit to connect to the FortiResponse Distribution Network (FDN) to update the antivirus and attack definitions and antivirus engine. You have the following update options:

- Request updates from the FDN manually,
- Schedule updates to automatically request the latest versions hourly, daily, or weekly
- Push updates so that the FDN contacts your FortiGate unit when a new update is available.

To receive scheduled updates and push updates, you must register the FortiGate unit on the Fortinet Support web page.

This chapter describes:

- [Updating antivirus and attack definitions](#)
- [Registering FortiGate units](#)
- [Updating registration information](#)
- [Registering a FortiGate unit after an RMA](#)

## Updating antivirus and attack definitions

You can configure the FortiGate unit to connect to the FortiResponse Distribution Network (FDN) to automatically receive the latest antivirus and attack definitions and antivirus engine updates. The FortiGate unit supports the following antivirus and attack definition update features:

- User-initiated manual updates from the FDN,
- Hourly, daily, or weekly scheduled antivirus and attack definition and antivirus engine updates from the FDN,
- Push updates from the FDN,
- View the update status including version numbers, expiry dates, and update dates and times,
- Push updates through a NAT device.

The System > Update page web-based manager displays the following antivirus and attack definition update information:

|                            |                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Version</b>             | Displays the current antivirus engine, virus definition, and attack definition version numbers.                                                                                                                                                                                                                                                                                      |
| <b>Expiry date</b>         | Displays the expiry date of your license for antivirus engine, virus definition, and attack definition updates.                                                                                                                                                                                                                                                                      |
| <b>Last update attempt</b> | Displays the date and time on which the FortiGate unit last attempted to download antivirus engine, virus definition, and attack definition updates.                                                                                                                                                                                                                                 |
| <b>Last update status</b>  | Displays the success or failure of the last update attempt. No updates means the last update attempt was successful but no new updates are available. Update succeeded or similar messages mean the last update attempt was successful and new updates were installed. Other messages can indicate that the FortiGate was not able to connect to the FDN and other error conditions. |

This section describes:

- [Connecting to the FortiResponse Distribution Network](#)
- [Configuring scheduled updates](#)
- [Configuring update logging](#)
- [Adding an override server](#)
- [Manually updating antivirus and attack definitions](#)
- [Configuring push updates](#)
- [Push updates through a NAT device](#)
- [Scheduled updates through a proxy server](#)

## Connecting to the FortiResponse Distribution Network

Before the FortiGate unit can receive antivirus and attack updates, it must be able to connect to the FortiResponse Distribution Network (FDN). The FortiGate unit uses HTTPS on port 8890 to connect to the FDN. The FortiGate external interface must have a path to the internet using port 8890. To configure scheduled updates, see [“Configuring scheduled updates” on page 93](#).

You can also configure the FortiGate unit to allow push updates. Push updates are provided to the FortiGate unit from the FDN using HTTPS on UDP port 9443. To receive push updates, the FDN must have a path to the FortiGate external interface using UDP port 9443. To configure push updates, see [“Configuring push updates” on page 95](#).

The FDN is a world-wide network of FortiResponse Distribution Servers (FDSs). When your FortiGate unit connects to the FDN it actually connects to the nearest FDS. To do this, all FortiGate units are programmed with a list of FDS addresses sorted by nearest time zone according to the time zone configured for the FortiGate unit. To make sure the FortiGate unit receives updates from the nearest FDS, go to **System > Config > Time** and make sure you have selected the correct time zone for your area.

To make sure the FortiGate unit can connect to the FDN:

- 1 Go to **System > Config > Time** and make sure the time zone is set to the correct time zone for your area.
- 2 Go to **System > Update**.
- 3 Select Refresh.

The FortiGate unit tests its connection to the FDN. The test results are displayed at the top of the System Update page.

**Table 1: Connections to the FDN**

| Connections                               | Status        | Comments                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FortiResponse Distribution Network</b> | Available     | The FortiGate unit can connect to the FDN. You can configure the FortiGate unit for scheduled updates. See <a href="#">"Configuring scheduled updates" on page 93</a> .                                                                                                                                                                                                                                                                                                                                                         |
|                                           | Not available | The FortiGate unit cannot connect to the FDN. You must configure your FortiGate unit and your network so that the FortiGate unit can connect to the Internet and to the FDN. For example, you may need to add routes to the FortiGate routing table or configure your network to allow the FortiGate unit to use HTTPS on port 8890 to connect to the Internet.<br>You may also have to connect to an override FortiResponse server to receive updates. See <a href="#">"Configuring update logging" on page 94</a> .           |
| <b>Push Update</b>                        | Available     | The FDN can connect to the FortiGate unit to send push updates. You can configure the FortiGate unit to receive push updates. See <a href="#">"Configuring push updates" on page 95</a> .                                                                                                                                                                                                                                                                                                                                       |
|                                           | Not available | The FDN cannot connect to the FortiGate unit to send push updates. Push updates may not be available if you have not registered the FortiGate unit (see <a href="#">"Registering the FortiGate unit" on page 102</a> ), if there is a NAT device installed between the FortiGate unit and the FDN (see <a href="#">"Push updates through a NAT device" on page 96</a> ), or if your FortiGate unit connects to the Internet using a proxy server (see <a href="#">"Scheduled updates through a proxy server" on page 100</a> ). |

## Configuring scheduled updates

You can configure the FortiGate unit to check for and download updated definitions hourly, daily, or weekly according to the schedule you specify.

- 1 Go to **System > Update**.
- 2 Select Scheduled Update.
- 3 Select whether to check for and download updates hourly, daily, or weekly:

**Hourly** Once every 1 to 23 hours. Select the number of hours and minutes between each update request.

**Daily** Once a day. You can specify the time of day to check for updates.

**Weekly** Once a week. You can specify the day of the week and the time of day to check for updates.

4 Select Apply.

The FortiGate unit starts the next scheduled update according to the new update schedule.

Whenever a scheduled update is run, the event is recorded in the FortiGate event log.

**Figure 1: Configuring automatic antivirus and attack definitions updates**

The screenshot shows the 'Update' configuration page in FortiGate. It includes a 'Refresh' button and a table of update details. Below the table, there are checkboxes for 'Allow Push Update' and 'Scheduled Update', along with fields for override IP, port, and update frequency.

| Update                | Version | Expiry date              | Last update attempt      | Last Update Status |
|-----------------------|---------|--------------------------|--------------------------|--------------------|
| Anti Virus Engine     | 1.00    | Mon Nov 29 19:00:00 1999 | Tue Aug 12 14:25:21 2003 | No updates         |
| Anti Virus Definition | 4.115   | Mon Nov 29 19:00:00 1999 | Tue Aug 12 14:25:21 2003 | No updates         |
| Attack Definition     | 2.56    | Mon Nov 29 19:00:00 1999 | Tue Aug 12 14:25:21 2003 | No updates         |

Below the table, the 'Allow Push Update' checkbox is checked. The 'Use override push IP' field is set to 64.230.123.149 and the Port is 45034. The 'Scheduled Update' checkbox is also checked. The update frequency is set to 'Every 1 (hour) 45 (minutes after the hour)'. There are 'Apply' and 'Update Now' buttons at the bottom.

## Configuring update logging

Use the following procedure to configure FortiGate logging to record log messages when the FortiGate unit updates antivirus and attack definitions. Update log messages are recorded on the FortiGate Event log.

- 1 Go to **Log&Report > Log Setting**.
- 2 Select Config Policy for the type of logs that the FortiGate unit is configured to record. See [“Recording logs” on page 249](#).
- 3 Select Update to record log messages when the FortiGate unit updates antivirus and attack definitions.
- 4 Select the following update log options:

|                          |                                                                                                                                       |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <b>Failed Update</b>     | The FortiGate unit records a log message whenever an update attempt fails.                                                            |
| <b>Successful Update</b> | The FortiGate unit records a log message whenever an update attempt is successful.                                                    |
| <b>FDN error</b>         | The FortiGate unit records a log message whenever it cannot connect to the FDN or whenever it receives an error message from the FDN. |

- 5 Select OK.

## Adding an override server

If you cannot connect to the FDN or if your organization provides antivirus and attack updates using their own FortiResponse server, you can use the following procedure to add the IP address of an override FortiResponse server.

- 1 Go to **System > Update**.
- 2 Select Use override server address and add the IP address of a FortiResponse server.
- 3 Select Apply.

The FortiGate unit tests the connection to the override server.

If the FortiResponse Distribution Network setting changes to available, the FortiGate unit has successfully connected to the override server.

If the FortiResponse Distribution Network stays set to not available, the FortiGate unit cannot connect to the override server. Check the FortiGate configuration and the network configuration to make sure you can connect to the override FortiResponse server from the FortiGate unit.

## Manually updating antivirus and attack definitions

You can use the following procedure to update the antivirus and attack definitions at any time. To run this procedure the FortiGate unit must be able to connect to the FDN or to an override FortiResponse server.

- 1 Go to **System > Update**.
- 2 Select Update Now to update the antivirus and attack definitions.

If the connection to the FDN or override server is successful, the web-based manager displays a message similar to the following:

Your update request has been sent. Your database will be updated in a few minutes. Please check your update page for the status of the update.

After a few minutes, if an update is available, the System Update page lists new version information for antivirus definitions, the antivirus engine, or for attack definitions. The System Status page will also display new dates and version numbers for antivirus and attack definitions. Messages are recorded to the event log indicating whether the update was successful or not.

## Configuring push updates

The FDN can push updates to FortiGate units to provide the fastest possible response to critical situations. You must register the FortiGate unit before it can receive push updates. See [“Registering the FortiGate unit” on page 102](#).

If the FDN must connect to the FortiGate unit through a NAT device, see [“Push updates through a NAT device” on page 96](#).

Push updates are not supported if the FortiGate unit must use a proxy server to connect to the FDN. See [“Scheduled updates through a proxy server” on page 100](#) for more information.

## To enable push updates

- 1 Go to **System > Update**.
- 2 Select Allow Push Update.
- 3 Select Apply.

## About push updates

When you configure a FortiGate unit to allow push updates, the FortiGate unit sends a SETUP message to the FDN. The next time a new antivirus engine, new antivirus definitions, or new attack definitions are released, the FDN notifies all FortiGate units configured for push updates that a new update is available. Within 60 seconds of receiving a push notification, the FortiGate unit attempts to request an update from the FDN.

If available for your network configuration, configuring push updates is recommended in addition to configuring scheduled updates. Push updates mean that on average the FortiGate unit receives new updates sooner than if the FortiGate just receives scheduled updates. However, scheduled updates make sure that the FortiGate unit does eventually receive the latest updates.

Enabling push updates is not recommended as the only method for obtaining updates. The push notification may not be received by the FortiGate unit. Also, when the FortiGate unit receives a push notification it will only make one attempt to connect to the FDN and download updates.

## Push updates and external dynamic IP addresses

If the external interface of the FortiGate unit is configured with a dynamic IP address (using PPPoE or DHCP), whenever the IP address of the external interface changes, a SETUP message is sent to the FDN to notify it of the change. As long as this SETUP message is sent, the FDN will have the most up-to-date IP address and the next push notification is sent to this IP address.

## Push updates through a NAT device

If the FDN can only connect to the FortiGate unit through a NAT device, you must configure port forwarding on the NAT device and add the port forwarding information to the push update configuration. Using port forwarding, the FDN connects to the FortiGate unit using either port 9443 or an override push port that you assign.



**Note:** You cannot receive push updates through a NAT device if the external IP address of the NAT device is dynamic (for example, set using PPPoE or DHCP).

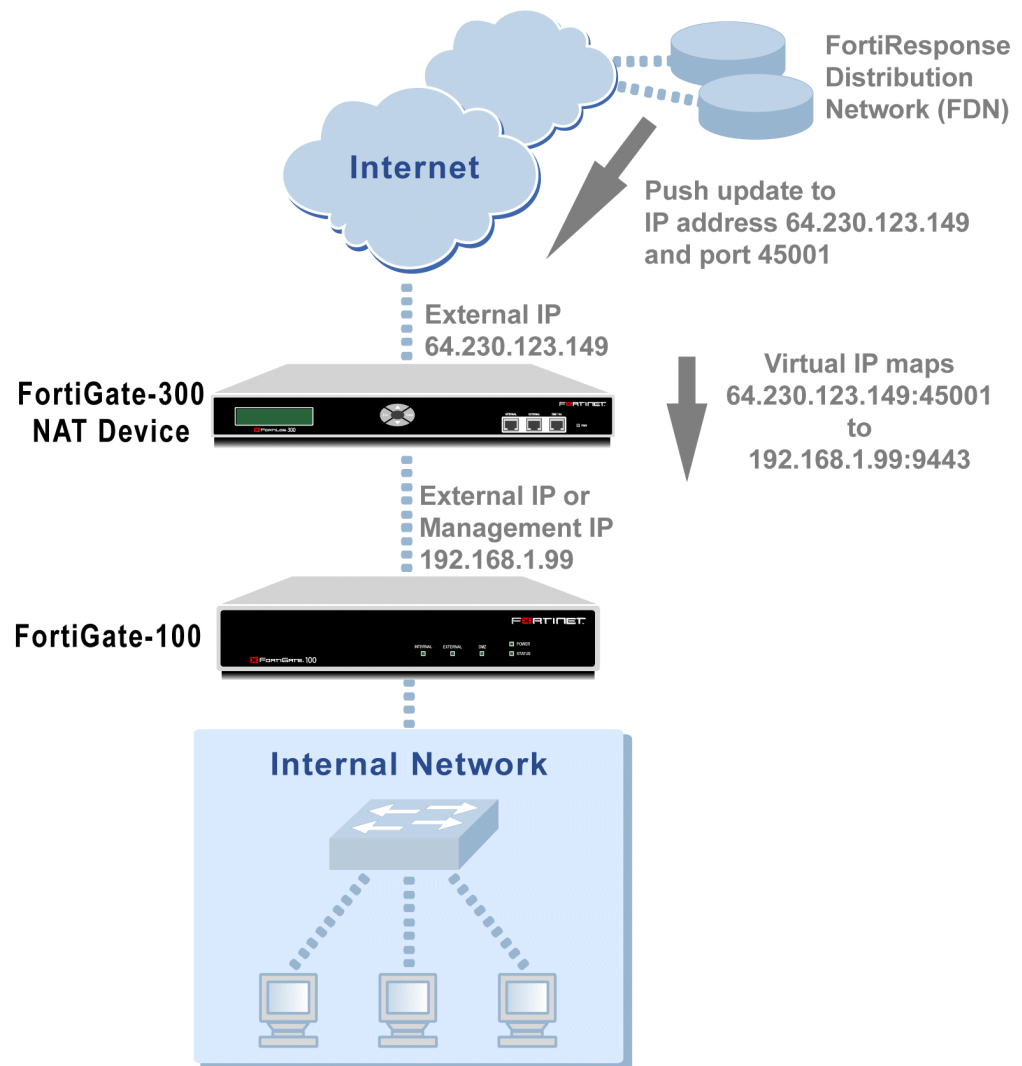
### Example: push updates through a NAT device

This example describes how to configure a FortiGate NAT device to forward push updates to a FortiGate unit installed on its internal network. For the FortiGate unit on the internal network to receive push updates, the FortiGate NAT device must be configured with a port forwarding virtual IP. This virtual IP maps the IP address of the external interface of the FortiGate NAT device and a custom port to the IP address of the FortiGate unit on the internal network. This IP address can either be the external IP address of the FortiGate unit if it is operating in NAT/Route mode or the Management IP address of the FortiGate unit if it is operating in Transparent mode.



**Note:** This example describes the configuration for a FortiGate NAT device. However, any NAT device with a static external IP address that can be configured for port forwarding can be used.

Figure 2: Example network topology: Push updates through a NAT device



### General procedure

Use the following steps to configure the FortiGate NAT device and the FortiGate unit on the Internal network so that the FortiGate unit on the Internal network can receive push updates:

- 1 Add a port forwarding virtual IP to the FortiGate NAT device.
- 2 Add a firewall policy to the FortiGate NAT device that includes the port forwarding virtual IP.
- 3 Configure the FortiGate unit on the internal network with an override push IP and port.



**Note:** Before completing the following procedure you should register the FortiGate unit on the internal network so that it can receive push updates.

### Adding a port forwarding virtual IP to the FortiGate NAT device

Use the following procedure to configure a FortiGate NAT device to use port forwarding to forward push update connections from the FDN to a FortiGate unit on the internal network.

To configure the FortiGate NAT device:

- 1 Go to **Firewall > Virtual IP**.
- 2 Select New.
- 3 Add a name for the virtual IP.
- 4 Select the External interface that the FDN connects to.  
For the example topology, select the external interface.
- 5 Select Port Forwarding.
- 6 Enter the External IP address that the FDN connects to.  
For the example topology, enter 64.230.123.149.
- 7 Enter the External Service Port that the FDN connects to.  
For the example topology, enter 45001.
- 8 Set Map to IP to the IP address of the FortiGate unit on the internal network.  
If the FortiGate unit is operating in NAT/Route mode, enter the IP address of the external interface.  
If the FortiGate unit is operating in Transparent mode, enter the management IP address.  
For the example topology, enter 192.168.1.99.
- 9 Set the Map to Port to 9443.
- 10 Set Protocol to UDP.
- 11 Select OK.

**Figure 3: Push update port forwarding virtual IP**

**Virtual IP**

**Add New Virtual IP Mapping**

Name: Push\_VIP

External Interface: external

Type: ☐ Static NAT ☒ Port Forwarding

External IP Address: 64.230.123.149

External Service Port: 45001

Map to IP: 192.168.1.99

Map to Port: 9443

Protocol: ☐ TCP ☒ UDP

OK Cancel

**Adding a firewall policy for the port forwarding virtual IP**

To configure the FortiGate NAT device:

- 1 Add a new external to internal firewall policy.
- 2 Configure the policy with the following settings:

|                    |                             |
|--------------------|-----------------------------|
| <b>Source</b>      | External_All                |
| <b>Destination</b> | The virtual IP added above. |
| <b>Schedule</b>    | Always                      |
| <b>Service</b>     | ANY                         |
| <b>Action</b>      | Accept                      |
| <b>NAT</b>         | Selected.                   |

- 3 Select OK.

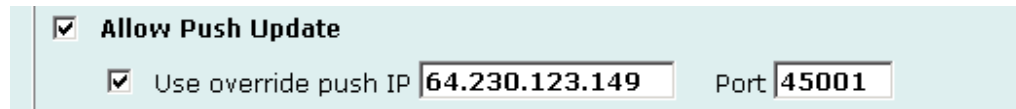
**Configure the FortiGate unit with an override push IP and port**

To configure the FortiGate unit on the internal network:

- 1 Go to **System > Update**.
- 2 Select Allow Push Update.
- 3 Select Use override push.
- 4 Set IP to the External IP Address added to the virtual IP.  
For the example topology, enter 64.230.123.149.

- 5 Set Port to the External Service Port added to the virtual IP.  
For the example topology, enter 45001.
- 6 Select Apply.  
The FortiGate unit sends the override push IP address and Port to the FDN. The FDN will now use this IP address and port for push updates to the FortiGate unit on the internal network.  
If the External IP Address or External Service Port change, add the changes to the Use override push configuration and select Apply to update the push information on the FDN.

**Figure 4: Example push update configuration**



☒ **Allow Push Update**

☒ Use override push IP  Port

- 7 Select Apply.
- 8 You can select Refresh to make sure that push updates work.  
Push Update should change to Available.

## Scheduled updates through a proxy server

If your FortiGate unit must connect to the Internet through a proxy server, you can use the `set system autoupdate tunneling` command to allow the FortiGate unit to connect (or tunnel) to the FDN using the proxy server. Using the command you can specify the IP address and port of the proxy server. As well, if the proxy server requires authentication, you can add the user name and password required for the proxy server to the autoupdate configuration. The full syntax for enabling updates through a proxy server is:

```
set system autoupdate tunneling enable [address
<proxy-address_ip> [port <proxy-port> [username <username_str>
[password <password_str>]]]]
```

For example, if the IP address of the proxy server is 64.23.6.89 and its port is 8080, enter the following command:

```
set system autoupdate tunneling enable address 64.23.6.89
port 8080
```

For more information about the `set system autoupdate` command, see *Volume 6, FortiGate CLI Reference Guide*.

The FortiGate unit connects to the proxy server using the HTTP CONNECT method, as described in RFC 2616. The FortiGate unit sends an HTTP CONNECT request to the proxy server (optionally with authentication information) specifying the IP address and port required to connect to the FDN. The proxy server establishes the connection to the FDN and passes information between the FortiGate unit and the FDN.

The CONNECT method is used mostly for tunneling SSL traffic. Some proxy servers won't allow the CONNECT to connect to just any port; they restrict the allowed ports to the well known ports for HTTPS and perhaps some other similar services. Because FortiGate autoupdates use HTTPS on port 8890 to connect to the FDN, your proxy server may have to be configured to allow connections on this port.

There are no special tunneling requirements if you have configured an override server address to connect to the FDN.

Push updates are not supported if the FortiGate must connect to the Internet through a proxy server.

## Registering FortiGate units

After purchasing and installing a new FortiGate unit, you can register the unit using the web-based manager by going to **System > Update > Support**, or by using a web browser to connect to <http://support.fortinet.com> and selecting Product Registration.

Registration consists of entering your contact information and the serial numbers of the FortiGate units you or your organization have purchased. Registration is quick and easy. You can register multiple FortiGate units in a single session without re-entering your contact information.

Once registration is completed, Fortinet sends a Support Login user name and password to your email address. You can use this user name and password to log on to the Fortinet support web site to:

- View your list of registered FortiGate units
- Register additional FortiGate units
- Add or change FortiCare Support Contract numbers for each FortiGate unit
- View and change registration information
- Download virus and attack definitions updates
- Download firmware upgrades
- Modify registration information after an RMA

Soon you will also be able to:

- Access Fortinet user documentation
- Access the Fortinet knowledge base

All registration information is stored in the Fortinet Customer Support database. This information is used to make sure that your registered FortiGate units can be kept up to date. All information is strictly confidential. Fortinet does not share this information with any third party organizations for any reason.

This section describes:

- [FortiCare Service Contracts](#)
- [Registering the FortiGate unit](#)

### FortiCare Service Contracts

Owners of a new FortiGate unit are entitled to 90 days of technical support services. To continue receiving support services after the 90 day expiry date, you must purchase a FortiCare Support Contract from an authorized Fortinet reseller or distributor. Different levels of service are available so you can purchase the support that you need. For maximum network protection, Fortinet strongly recommends that all customers purchase a service contract that covers antivirus and attack definition updates. See your Fortinet reseller or distributor for details of packages and pricing.

To activate the FortiCare Support Contract, you must register the FortiGate unit and add the FortiCare Support Contract number to the registration information. You can also register the FortiGate unit without purchasing a FortiCare Support Contract. In this case, when you do purchase a FortiCare Support Contract you can update the registration information to add the support contract number.

A single FortiCare Support Contract can cover multiple FortiGate units. You must enter the same service contract number for each of the FortiGate models covered by the service contract.

## Registering the FortiGate unit

Before registering a FortiGate unit, you require the following information:

- Your contact information including:
  - First and last name
  - Company name
  - Email address (Your Fortinet support login user name and password will be sent to this email address.)
  - Address
  - Contact phone number
- A security question and an answer to the security question.

This information is used for password recovery. The security question should be a simple question that only you know the answer to. The answer should not be easy to guess.
- The product model and serial number for each FortiGate unit to be registered.

The serial number is located on a label on the bottom of the FortiGate unit.

You can view the Serial number from the web-based manager by going to System > Status.

The serial number is also available from the CLI using the `get system status` command.
- FortiCare Support Contract numbers if you have purchased FortiCare Support Contracts for the FortiGate units to be registered.

### To register one or more FortiGate units

- 1 Go to **System > Update > Support**.
- 2 Enter your contact information into the product registration form.

**Figure 5: Registering a FortiGate unit (contact information and security question)**

| Contact Information           |                                                              |                  |               |
|-------------------------------|--------------------------------------------------------------|------------------|---------------|
| First Name *                  | Customer                                                     | Last Name *      | Name          |
| Company *                     | Company                                                      | Title            | Administrator |
| Email *                       | Customer@company.com                                         |                  |               |
| Address 1 *                   | 123 My Street                                                |                  |               |
| Address 2                     |                                                              |                  |               |
| City *                        | City                                                         | State/Province * | State         |
| Zip *                         | 123456                                                       | Country/Region * | UNITED STATES |
| Contact Phone *               | 1-555-555-5555                                               | Fax Number       |               |
| Security Question *           | Security question (will be used if you forgot your password) |                  |               |
| Answer to Security Question * | ***** (will be used if you forgot your password)             |                  |               |

- 3 Provide a security question and an answer to the security question.
- 4 Select the model number of the Product Model to register.
- 5 Enter the Serial Number of the FortiGate unit.
- 6 If you have purchased a FortiCare Support Contract for this FortiGate unit, enter the support contract number.

**Figure 6: Registering a FortiGate unit (product information)**

| Product Information  |                                                                                                      |
|----------------------|------------------------------------------------------------------------------------------------------|
| Product Model *      | FGT-60                                                                                               |
| Serial Number *      | FGT-60280303002<br>(Located on bottom of unit and also on "System" screen on the web user interface) |
| Support Contract No. | 334278334744                                                                                         |

**\* - indicates Required Fields**

- 7 Select Finish.  
 If you have not entered a FortiCare Support Contract number (SCN) you can return to the previous page to enter the number. If you do not have a FortiCare Support Contract you can select Continue to complete the registration.  
 If you have entered a support contract number a real-time validation is performed to verify that the SCN information matches the FortiGate unit. If the information doesn't match you can try entering it again.  
 A web page is displayed that contains detailed information about the Fortinet technical support services available to you for the registered FortiGate unit.  
 Your Fortinet support user name and password is sent to the email address provided with your Contact information.

## Updating registration information

You can use your Fortinet support user name and password to log on to the Fortinet Support web site at any time to view or update your Fortinet support information.

This section describes:

- [Recovering a lost Fortinet support password](#)
- [Viewing the list of registered FortiGate units](#)
- [Registering a new FortiGate unit](#)
- [Adding or changing a FortiCare Support Contract number](#)
- [Changing your Fortinet support password](#)
- [Changing your contact information or security question](#)
- [Downloading virus and attack definitions updates](#)

### Recovering a lost Fortinet support password

If you provided a security question and answer when you registered on the Fortinet support web site, you can use the following procedure to receive a replacement password. If you did not provide a security question and answer, contact Fortinet tech support.

- 1 Go to **System > Update > Support**.
- 2 Select Support Login.
- 3 Enter your Fortinet support user name.
- 4 Select Forgot your password?
- 5 Enter your email address and select Submit.

The security question that you entered when you registered is displayed.

- 6 Enter the answer to your security question and select Get Password.

If you entered the correct answer to the security question, an email containing a new password is sent to your email address. You can use your current user name and this password to log into the Fortinet support web site.

- 7 Select Support Login.
- 8 When your new password arrives, enter your user name and new password to log into the Fortinet support web site.

### Viewing the list of registered FortiGate units

- 1 Go to **System > Update > Support** and select Support Login.
- 2 Enter your Fortinet support user name and password.
- 3 Select Login.
- 4 Select View Products.

The list of FortiGate products that you have registered is displayed. For each FortiGate unit, the list includes the serial number and current support options for that unit.

**Figure 7: Sample list of registered FortiGate units**

| View Product Support                  |       |                 |                 |
|---------------------------------------|-------|-----------------|-----------------|
| <b>Serial Number</b> FGT-602803030020 |       |                 |                 |
| Support Type                          | Hours | Activation Date | Expiration Date |
| Hardware Coverage                     | --    | 5/12/2003       | 5/11/2004       |
| Firmware Updates                      | --    | 5/12/2003       | 8/10/2003       |
| Telephone Support                     | 8x5   | 5/12/2003       | 8/10/2003       |
| Virus Definitions Updates             | --    | 5/12/2003       | 8/10/2003       |
| Attack Definitions Updates            | --    | 5/12/2003       | 8/10/2003       |
| <b>Serial Number</b> FGT1002801021024 |       |                 |                 |
| Support Type                          | Hours | Activation Date | Expiration Date |
| Hardware Coverage                     | --    | 5/7/2003        | 5/6/2004        |
| Firmware Updates                      | --    | 5/7/2003        | 8/5/2003        |
| Telephone Support                     | 8x5   | 5/7/2003        | 8/5/2003        |
| Virus Definitions Updates             | --    | 5/7/2003        | 8/5/2003        |
| Attack Definitions Updates            | --    | 5/7/2003        | 8/5/2003        |

## Registering a new FortiGate unit

- 1 Go to **System > Update > Support** and select Support Login.
- 2 Enter your Fortinet support user name and password.
- 3 Select Login.
- 4 Select Add Registration.
- 5 Select the model number of the Product Model to register.
- 6 Enter the Serial Number of the FortiGate unit.
- 7 If you have purchased a FortiCare Support Contract for this FortiGate unit, enter the support contract number.
- 8 Select Finish.

The list of FortiGate products that you have registered is displayed. The list now includes the new FortiGate unit.

## Adding or changing a FortiCare Support Contract number

- 1 Go to **System > Update > Support** and select Support Login.
- 2 Enter your Fortinet support user name and password.
- 3 Select Login.
- 4 Select Add/Change Contract number.
- 5 Select the Serial Number of the FortiGate unit for which to add or change a FortiCare Support Contract number.
- 6 Add the new Support Contract number.

- 7 Select Finish.

The list of FortiGate products that you have registered is displayed. The list now includes the new support contract information.

## Changing your Fortinet support password

- 1 Go to **System > Update > Support** and select Support Login.
- 2 Enter your Fortinet support user name and password.
- 3 Select Login.
- 4 Select My Profile.
- 5 Select Change Password.
- 6 Enter your current password.
- 7 Enter and confirm a new password.

An email is sent to your email address confirming that your password has been changed. Use your current user name and new password the next time you log into the Fortinet tech support web site.

## Changing your contact information or security question

- 1 Go to **System > Update > Support** and select Support Login.
- 2 Enter your Fortinet support user name and password.
- 3 Select Login.
- 4 Select My Profile.
- 5 Select Edit Profile.
- 6 Make the required changes to your contact information.
- 7 Make the required changes to your security question and answer.
- 8 Select Update Profile.

Your changes are saved to the Fortinet technical support database. If you changed your contact information, the changes are displayed.

## Downloading virus and attack definitions updates

Use the following procedure to manually download virus and attack definitions updates. This procedure also describes how to install the definitions updates on your FortiGate unit.

- 1 Go to **System > Update > Support** and select Support Login.
- 2 Enter your Fortinet support user name and password.
- 3 Select Login.
- 4 Select Download Virus/Attack Update.
- 5 If required, select the FortiOS version.
- 6 Select the virus and attack definitions to download.

Figure 8: Downloading virus and attack definition updates

| Download Virus/Attack Updates        |                  |                   |
|--------------------------------------|------------------|-------------------|
| Version: <b>v2.36</b>   <b>v2.30</b> |                  |                   |
| FGT Unit                             | Virus Definition | Attack Definition |
| FGT-50                               | OS2.3.6_4.77.    | 2.36-1.41         |
| FGT-60                               |                  | 2.36-1.41         |
| FGT-100                              | OS2.3.6_4.77.    | 2.36-1.41         |
| FGT-200                              | OS2.3.6_4.77.    | 2.36-1.41         |
| FGT-300                              | OS2.3.6_4.77.    | 2.36-1.41         |
| FGT-400                              | OS2.3.6_4.77.    | 2.36-1.41         |
| FGT-500                              | OS2.3.6_4.77.    | 2.36-1.41         |
| FGT-1000                             |                  | 2.36-1.41         |
| FGT-3000                             | OS2.3.6_4.77.    | 2.36-1.41         |
| FGT-3600                             |                  | 2.36-1.41         |

For information about how to install the downloaded files, see [“Manual virus definition updates” on page 82](#) and [“Manual attack definition updates” on page 83](#).

## Registering a FortiGate unit after an RMA

The Return Material Authorization (RMA) process starts when a customer's registered FortiGate unit doesn't work properly due to a hardware failure. If this happens while the FortiGate unit is still protected by hardware coverage, you can return the FortiGate unit that is not functioning to your reseller or distributor.

The RMA is recorded and you will receive a replacement unit. Fortinet adds the RMA information to the Fortinet support database. When you receive the replacement unit you can use the following procedure to update your product registration information.

- 1 Go to **System > Update > Support** and select Support Login.
- 2 Enter your Fortinet support user name and password to log in.
- 3 Select Add Registration.
- 4 Select the link to replace a unit with a new unit from an RMA.
- 5 Select Finish.

The list of FortiGate products that you have registered is displayed. The list now includes the replacement FortiGate unit. All support levels are transferred to the replacement unit.





# Network configuration

Go to **System > Network** to make any of the following changes to the FortiGate network settings:

- [Configuring interfaces](#)
- [Adding DNS server IP addresses](#)
- [Configuring routing](#)
- [Providing DHCP services to your internal network](#)

## Configuring interfaces

Use the following procedures to configure interfaces:

- [Viewing the interface list](#)
- [Bringing up an interface](#)
- [Changing an interface static IP address](#)
- [Adding a secondary IP address to an interface](#)
- [Adding a ping server to an interface](#)
- [Controlling management access to an interface](#)
- [Configuring traffic logging for connections to an interface](#)
- [Configuring the external interface with a static IP address](#)
- [Configuring the external interface for DHCP](#)
- [Configuring the external interface for PPPoE](#)
- [Changing the external interface MTU size to improve network performance](#)
- [Configuring the management interface \(Transparent mode\)](#)

## Viewing the interface list

Use the following procedure to view the interface list.

- 1 Go to **System > Interface**.

The interface list is displayed. The interface list shows the following status information for all of the FortiGate interfaces:

- The IP address of the interface
- The netmask of the interface
- The administrative access configuration for the interface
- The link status for the interface

If the link status is a green arrow, the interface is up and can accept network traffic.

If the link status is a red arrow, the interface is down and cannot accept traffic. To bring an interface up, see the procedure [“Bringing up an interface”](#).

## Bringing up an interface

If the link status of an interface on the interface shows that it is down, you can use the following procedure to bring the interface up.

- 1 Go to **System > Interface**.  
The interface list is displayed.
- 2 Select Bring Up for the interface that you want to bring up.

## Changing an interface static IP address

Use the following procedure to change the static IP address of any FortiGate interface. You can also use this procedure to add an IP address to an interface.

- 1 Go to **System > Network > Interface**.
- 2 Select Modify  for the interface to change.
- 3 Change the IP address and Netmask as required.

The IP address of the interface must be on the same subnet as the network the interface is connecting to.

Two interfaces cannot have the same IP address and cannot have IP addresses on the same subnet.

- 4 Select OK to save your changes.

If you changed the IP address of the interface that you are connecting to manage the FortiGate unit, you must reconnect to the web-based manager using the new interface IP address.

## Adding a secondary IP address to an interface

You can use the CLI to add a secondary IP address to any FortiGate interface. The secondary IP address cannot be the same as the primary IP address but it can be on the same subnet.

To add a secondary IP address from the CLI enter the command:

```
set system interface internal config secip <second_ip>
<netmask_ip>
```

You can also configure management access and add a ping server to the secondary IP address.

```
set system interface <intf_str> config secallowaccess ping
https ssh snmp http telnet
set system interface <intf_str> config secgwdetect enable
```

## Adding a ping server to an interface

Add a ping server to an interface if you want the FortiGate unit to confirm connectivity with the next hop router on the network connected to the interface. Adding a ping server is required for routing failover. See [“Adding destination-based routes to the routing table” on page 116](#).

- 1 Go to **System > Network > Interface**.
- 2 Select Modify  for the interface to which to add a Ping server.
- 3 Set Ping Server to the IP address of the next hop router on the network connected to the interface.
- 4 Select Enable.  
The FortiGate unit uses dead gateway detection to ping the Ping Server IP address to make sure that the FortiGate unit can connect to the this IP address. To configure dead gateway detection, see [“To modify the Dead Gateway Detection settings” on page 131](#).
- 5 Select OK to save your changes.

## Controlling management access to an interface

- 1 Go to **System > Network > Interface**.
- 2 Select Modify  for the interface for which to configure management access.
- 3 Select the management Access methods for the interface.
 

|               |                                                                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HTTPS</b>  | To allow HTTPS connections to the web-based manager through this interface.                                                                         |
| <b>PING</b>   | If you want this interface to respond to pings. Use this setting to verify your installation and for testing.                                       |
| <b>HTTP</b>   | To allow HTTP connections to the web-based manager through this interface. HTTP connections are not secure and can be intercepted by a third party. |
| <b>SSH</b>    | To allow secure SSH connections to the CLI through this interface.                                                                                  |
| <b>SNMP</b>   | To allow a remote SNMP manager to request SNMP information by connecting to this interface. See <a href="#">“Configuring SNMP” on page 134</a> .    |
| <b>TELNET</b> | To allow Telnet connections to the CLI through this interface. Telnet connections are not secure and can be intercepted by a third party.           |

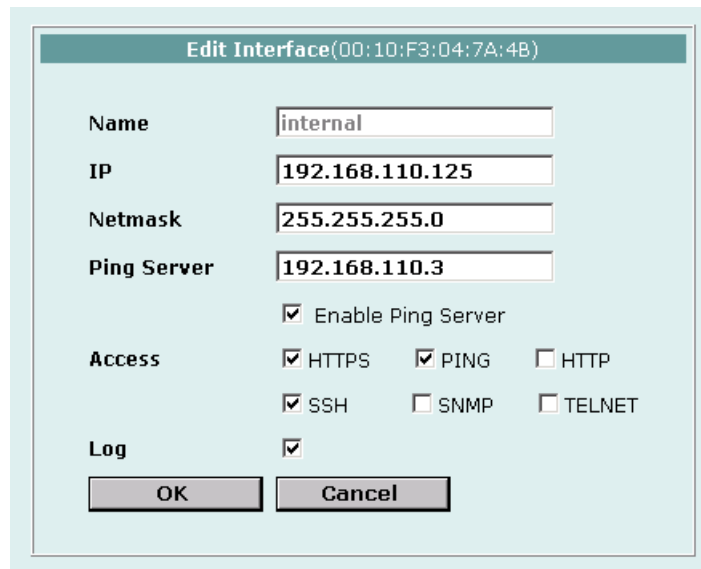
Configuring management access for an interface connected to the Internet allows remote administration of the FortiGate unit from any location on the Internet. Allowing management access from the Internet could compromise the security of your FortiGate unit. You should avoid allowing management access for an interface connected to the Internet unless this is required for your configuration. To improve the security of a FortiGate unit that allows remote management from the Internet, add secure administrative user passwords, change these passwords regularly, and only enable secure management access using HTTPS or SSH.

- 4 Select OK to save your changes.

## Configuring traffic logging for connections to an interface

- 1 Go to **System > Network > Interface**.
- 2 Select Modify  for the interface for which to configure logging.
- 3 Select Log to record log messages whenever a firewall policy accepts a connection to this interface.
- 4 Select OK to save your changes.

**Figure 1: Configuring the internal interface**



The screenshot shows the 'Edit Interface' window for the internal interface. The title bar reads 'Edit Interface(00:10:F3:04:7A:4B)'. The configuration fields are as follows:

| Field              | Value                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------|
| Name               | internal                                                                                                         |
| IP                 | 192.168.110.125                                                                                                  |
| Netmask            | 255.255.255.0                                                                                                    |
| Ping Server        | 192.168.110.3                                                                                                    |
| Enable Ping Server | <input checked="" type="checkbox"/>                                                                              |
| Access             | <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input type="checkbox"/> HTTP |
|                    | <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET            |
| Log                | <input checked="" type="checkbox"/>                                                                              |

At the bottom are 'OK' and 'Cancel' buttons.

## Configuring the external interface with a static IP address

- 1 Go to **System > Network > Interface**.
- 2 For the external interface, select Modify .
- 3 Set Addressing mode to Manual.
- 4 Change the IP address and Netmask as required.
- 5 Select OK to save your changes.

## Configuring the external interface for DHCP

Use the following procedure to configure the external interface to use DHCP. This configuration is required if your ISP uses DHCP to assign the IP address of the external interface.

- 1 Go to **System > Network > Interface**.
- 2 For the external interface, select Modify .
- 3 Set Addressing mode to DHCP and select OK to change to DHCP mode. Both the IP address and Netmask change to 0.0.0.0.

- 4 Select **Connect to DHCP server** to automatically connect to a DHCP server.  
If you do not select **Connect to DHCP server**, the FortiGate unit will not connect to a DHCP server. You can deselect this option if you are configuring the FortiGate unit offline.
- 5 Select **OK**.  
The FortiGate unit attempts to contact a DHCP server from the external interface to set the external IP address, netmask, and default gateway IP address. When the FortiGate unit gets this information from the DHCP server, the new addresses and netmask are displayed in the IP address and Netmask fields.

## Configuring the external interface for PPPoE

Use the following procedure to configure the external interface to use PPPoE. This configuration is required if your ISP uses PPPoE to assign the IP address of the external interface.

- 1 Go to **System > Network > Interface**.
- 2 For the external interface, select **Modify** .
- 3 Set Addressing mode to PPPoE and select **OK** to change to PPPoE mode.
- 4 Enter your PPPoE account user name and password.
- 5 Select **OK**.  
The FortiGate unit attempts to contact the PPPoE server to set the external IP address, netmask, and default gateway IP address. When the FortiGate unit gets this information from the PPPoE server, the new addresses and netmask are displayed in the external IP address and netmask fields. If the PPPoE connection with your ISP is dropped, the FortiGate unit automatically attempts to re-establish the connection.
- 6 Select **Connect to PPPoE server** to automatically connect to the PPPoE server.
- 7 Select **OK**.

## Changing the external interface MTU size to improve network performance

To improve the performance of your Internet connection, you can adjust the maximum transmission unit (MTU) of the packets that the FortiGate unit transmits from its external interface. Ideally, you want this MTU to be the same as the smallest MTU of all the networks between the FortiGate unit and the Internet. If the packets that the FortiGate unit sends are larger, they get broken up or fragmented, which slows down transmission speeds.

Trial and error is the only sure way of finding the optimal MTU, but there are some guidelines that can help. For example, the MTU of many PPP connections is 576, so if you connect to the Internet via PPP or PPPoE, you might want to set the MTU size to 576. DSL modems also have small MTU sizes. Most Ethernet networks have an MTU of 1500.



**Note:** If you connect to your ISP using DHCP to obtain an IP address for the external interface, you cannot set the MTU below 576 bytes due to DHCP communication standards.



**Note:** You cannot set MTU size if the external interface is configured using PPPoE. The PPPoE protocol configures optimum MTU size.

To change the MTU size of the packets leaving the external interface:

- 1 Go to **System > Network > Interface**.
- 2 For the external interface, select Modify .
- 3 Select Fragment outgoing packets greater than MTU.
- 4 Set the MTU size.

Set the maximum packet size in the range of 68 to 1500 bytes. The default MTU size is 1500. Experiment by lowering the MTU to find an MTU size for best network performance.

## Configuring the management interface (Transparent mode)

In Transparent mode, you can configure the management interface for management access to the FortiGate unit.

- 1 Go to **System > Network > Management**.
- 2 Change the Management IP and Mask as required.  
This must be a valid address for the network from which you will manage the FortiGate unit.
- 3 Add a default gateway IP address if the FortiGate unit must connect to a default gateway to reach the management computer.
- 4 Select the management Access methods for each interface.  
By default in Transparent mode, you manage the FortiGate unit by connecting to the internal or dmz interface. However, you can configure the management interface so that you can manage the FortiGate unit by connecting to any interface.

|               |                                                                                                                                                             |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HTTPS</b>  | To allow secure HTTPS connections to the web-based manager using the management interface.                                                                  |
| <b>PING</b>   | If you want the management interface to respond to pings. Use this setting to verify your installation and for testing.                                     |
| <b>HTTP</b>   | To allow HTTP connections to the web-based manager using the management interface. HTTP connections are not secure and can be intercepted by a third party. |
| <b>SSH</b>    | To allow secure SSH connections to the CLI using the management interface.                                                                                  |
| <b>SNMP</b>   | To allow a remote SNMP manager to request SNMP information by connecting to the management interface. See <a href="#">"Configuring SNMP" on page 134</a> .  |
| <b>TELNET</b> | To allow Telnet connections to the CLI using the management interface. Telnet connections are not secure and can be intercepted by a third party.           |

- 5 Select Apply to save your changes.

**Figure 2: Configuring the management interface**

**Management IP:**  
IP  Mask

**Access:**

|          |                                           |                                          |                              |                               |                               |                                 |
|----------|-------------------------------------------|------------------------------------------|------------------------------|-------------------------------|-------------------------------|---------------------------------|
| internal | <input checked="" type="checkbox"/> HTTPS | <input checked="" type="checkbox"/> PING | <input type="checkbox"/> SSH | <input type="checkbox"/> SNMP | <input type="checkbox"/> HTTP | <input type="checkbox"/> TELNET |
| external | <input type="checkbox"/> HTTPS            | <input checked="" type="checkbox"/> PING | <input type="checkbox"/> SSH | <input type="checkbox"/> SNMP | <input type="checkbox"/> HTTP | <input type="checkbox"/> TELNET |
| dmz      | <input checked="" type="checkbox"/> HTTPS | <input checked="" type="checkbox"/> PING | <input type="checkbox"/> SSH | <input type="checkbox"/> SNMP | <input type="checkbox"/> HTTP | <input type="checkbox"/> TELNET |

## Adding DNS server IP addresses

Several FortiGate functions, including sending email alerts and URL blocking, use DNS.

To set the DNS server addresses:

- 1 Go to **System > Network > DNS**.
- 2 Change the primary and secondary DNS server addresses as required.
- 3 Select Apply to save your changes.

## Configuring routing

This section describes how to configure FortiGate routing. You can configure routing to add static routes from the FortiGate unit to local routers. Using policy routing you can increase the flexibility of FortiGate routing to support more advanced routing functions.

You can also use routing to create a multiple Internet connection configuration that supports redundancy and load sharing between the two Internet connections.

This section describes:

- [Adding a default route](#)
- [Adding destination-based routes to the routing table](#)
- [Adding routes in Transparent mode](#)
- [Configuring the routing table](#)
- [Policy routing](#)

## Adding a default route

Use the following procedure to add a default route for network traffic leaving the external interface.

- 1 Go to **System > Network > Routing Table**.
- 2 Select New to add a new route.
- 3 Set the Source IP and Netmask to 0.0.0.0.
- 4 Set the Destination IP and Netmask to 0.0.0.0.
- 5 Set Gateway 1 to the IP address of the routing gateway that routes traffic to the Internet.
- 6 Select OK to save the default route.



**Note:** Only 1 default route can be active at any 1 time. If two default routes are added to the routing table, only the default route closest to the top of the routing table is active.

## Adding destination-based routes to the routing table

Use the following procedure to add destination-based routes to the FortiGate routing table. Add destination-based routes to control the destination of traffic exiting the FortiGate unit. You configure routes by adding destination IP addresses and netmasks and adding gateways for these destination addresses. The gateways are the next hop routers to which to route traffic that matches the destination addresses in the route.

You can add one or two gateways to a route. If you add one gateway, the FortiGate unit routes the traffic to that gateway. You can add a second gateway to route traffic to the second gateway if the first gateway fails.

To support routing failover, the IP address of each gateway must be added to the ping server of the interface connected to the same network as the gateway. See [“Adding a ping server to an interface” on page 111](#).

### Adding destination-based routes to the routing table

- 1 Go to **System > Network > Routing Table**.
- 2 Select New to add a new route.
- 3 Type the Destination IP address and netmask for the route.
- 4 Add the IP address of Gateway #1.  
  
Gateway #1 is the IP address of the primary destination for the route.  
Gateway #1 must be on the same subnet as a Fortigate interface.  
If you are adding a static route from the FortiGate unit to a single destination router, you only need to specify one gateway.
- 5 Optionally, add the IP address of Gateway #2 if want to route traffic to multiple gateways.

- 6 Set Device #1 to the FortiGate interface through which to route traffic to connect to Gateway #1.

You can select the name of an interface or Auto (the default). If you select the name of an interface, the traffic is routed to that interface. If you select Auto the system selects the interface according to the following rules:

- If the Gateway #1 IP address is on the same subnet as a FortiGate interface, the system sends the traffic to that interface.
- If the Gateway #1 IP address is not on the same subnet as a FortiGate interface, the system routes the traffic to the external interface, using the default route.

You can use Device #1 to send packets to an interface that is on a different subnet than the destination IP address of the packets without routing them using the default route.

- 7 Set Device #2 to the FortiGate interface through which to route traffic to connect to Gateway #2.

You can select the name of an interface or Auto (the default). If you select the name of an interface, the traffic is routed to that interface. If you select Auto the system selects the interface according to rules:

- If the Gateway #2 IP address is on the same subnet as a FortiGate interface, the system sends the traffic to that interface.
- If the Gateway #2 IP address is not on the same subnet as a FortiGate interface, the system routes the traffic to the external interface, using the default route.

You can use Device #2 to send packets to an interface that is on a different subnet than the destination IP address of the packets without routing them using the default route.

- 8 Select OK to save the route.



**Note:** Any 2 routes in the routing table must differ by something other than just the gateway to be simultaneously active. If two routes added to the routing table are identical except for their gateway IP addresses, only the route closer to the top of the routing table can be active.



**Note:** Arrange routes in the routing table from more specific to more general. To arrange routes in the routing table, see ["Configuring the routing table"](#).

## Adding routes in Transparent mode

Use the following procedure to add routes when operating the FortiGate unit in Transparent mode.

- 1 Go to **System > Network > Routing**.
- 2 Select New to add a new route.
- 3 Enter the Destination IP address and Netmask for the route.
- 4 Enter the Gateway IP address for the route.
- 5 Select OK to save the new route.
- 6 Repeat these steps to add more routes as required.

## Configuring the routing table

The routing table shows the destination IP address and mask of each route you add as well as the gateways and devices added to the route. The routing table also displays the gateway connection status. A green check mark indicates that the FortiGate unit has used the ping server and dead gateway detection to determine that it can connect to the gateway; a red X means that a connection cannot be established. A blue question mark means that the connection status is unknown. For more information, see [“Adding a ping server to an interface” on page 111](#), and

The FortiGate unit assigns routes by searching for a match starting at the top of the routing table and moving down until it finds the first match. You must arrange routes in the routing table from more specific to more general. The default route is the most general route. If you add a default route, it should be at the bottom of the routing table.

- 1 Go to **System > Network > Routing Table**.
- 2 Choose a route to move and select Move to  to change its order in the routing table.
- 3 Type a number in the Move to field to specify where in the routing table to move the route and select OK.
- 4 Select Delete  to remove a route from the routing table.

**Figure 3: Routing table**

| IP         | Mask          | Gateway #1                                                                                          | Gateway #2                                                                                        | Device #1 | Device #2 | Modify                                                                                                                                                                                                                                                            |
|------------|---------------|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.10.10.0 | 255.255.255.0 | 120.45.67.1    |                                                                                                   | external  |           |    |
| 0.0.0.0    | 0.0.0.0       | 64.230.129.22  | 120.45.67.1  | external  |           |    |

## Policy routing

Policy routing extends the functions of destination routing. Using policy routing you can route traffic based not only the destination address but also on:

- Source address
- Protocol, service type, or port range
- Incoming or source interface

Using policy routing you can build a routing policy database (RPDB) that selects the appropriate route for traffic by executing a set of routing rules. To select a route for traffic the FortiGate unit matches the traffic with the policy routes added to the RPDB starting at the top of the list. The first policy route to match the traffic is used to set the route for the traffic. The route supplies the next hop gateway as well as the FortiGate interface to be used by the traffic.

Packets are matched with policy routes before they are matched with destination routes. If a packet does not match a policy route it is routed using destination routes.

The gateway added to a policy route must also be added to a destination route. When the FortiGate unit matches packets with a route in the RPDB, the FortiGate unit looks in the destination routing table for the gateway that was added to the policy route. If a match is found, the FortiGate routes the packet using the matched destination route. If a match is not found, the FortiGate routes the packet using normal routing.

To find a route with a matching gateway, the FortiGate unit starts at the top of the destination routing table and searches until it finds the first matching destination route. This matched route is used to route the packet.

## Policy routing command syntax

Configure policy routing using the following CLI command.

```
set system route policy <route_int> src <source_ip>
<source_mask> iifname <source-interface_name>
dst <destination_ip> <destination_mask>
oifname <destination-interface_name> protocol <protocol_int>
port <low-port_int> <high-port_int> gw <gateway_ip>
```

Complete policy routing command syntax is described in the *FortiGate CLI Reference Guide*.

## Providing DHCP services to your internal network

If the FortiGate unit is operating in NAT/Route mode, you can configure it to be the DHCP server for your internal network:

- 1 Go to **System > Network > DHCP**.
- 2 Select Enable DHCP.
- 3 Configure DHCP server settings.

|                        |                                                                                                                                                                                      |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Starting IP</b>     | Enter Starting IP and Ending IP to configure the range of IP addresses that the FortiGate unit can assign to DHCP clients. The addresses must be addresses on your internal network. |
| <b>Ending IP</b>       |                                                                                                                                                                                      |
| <b>Netmask</b>         | Enter the Netmask that the FortiGate unit assigns to the DHCP clients.                                                                                                               |
| <b>Lease Duration</b>  | Enter the interval in seconds after which a DHCP client must ask the DHCP server for a new address. The lease duration must be between 300 and 8000000 seconds.                      |
| <b>Domain</b>          | Optionally enter in the domain that the DHCP server assigns to the DHCP clients.                                                                                                     |
| <b>DNS IP</b>          | Enter the IP addresses of up to 3 DNS servers that the DHCP clients can use for looking up domain names.                                                                             |
| <b>Default Route</b>   | Enter the default route to be assigned to DHCP clients. The default route should be on the same subnet as the starting and ending IP addresses.                                      |
| <b>WINS</b>            | Add the IP addresses of one or two WINS servers to be assigned to DHCP clients.                                                                                                      |
| <b>Exclusion Range</b> | Optionally enter up to 4 exclusion ranges of IP addresses within the starting IP and ending IP addresses that cannot be assigned to DHCP clients.                                    |

- 4 Select Apply.
- 5 Configure the IP network settings of the computers on your network to obtain an IP address automatically using DHCP.

Figure 4: Sample DHCP settings

Enable DHCP ☒

Starting IP

Ending IP

Netmask

Lease Duration  (300-8000000 secs)

Domain

DNS IP

Default Route

WINS

Exclusion Range:

Range 1  -

Range 2  -

Range 3  -

Range 4  -

## Viewing the dynamic IP list

If you have configured the FortiGate unit as a DHCP server, you can view a list of IP addresses that the DHCP server has added, their corresponding MAC addresses, and the expiry time and date for these addresses. The FortiGate unit adds these addresses to the dynamic IP/MAC list and if IP/MAC binding is enabled, the addresses in the dynamic IP/MAC list are added to the list of trusted IP/MAC address pairs. For more information about IP/MAC binding, see [“IP/MAC binding” on page 166](#).

To view the dynamic IP list:

- 1 Go to **System > Network > DHCP**.
- 2 Select Dynamic IP List.

The dynamic IP list is displayed.

Figure 5: Example Dynamic IP list

| IP           | MAC               | Expire                   |
|--------------|-------------------|--------------------------|
| 192.168.2.20 | 00:60:67:3d:16:da | Sun Sep 22 19:52:21 2002 |
| 192.168.2.21 | 00:90:27:88:94:ab | Sun Sep 22 19:45:19 2002 |
| 192.168.2.22 | 00:e0:98:75:21:21 | Sun Sep 22 19:51:08 2002 |

# RIP configuration

The FortiGate implementation of the Routing Information Protocol (RIP) supports both RIP version 1 (as defined by RFC 1058) and RIP version 2 (also called RIP2 and defined by RFC 2453). RIP2 enables RIP messages to carry more information and support simple authentication. RIP2 also supports subnet masks, a feature not available in RIP.

RIP sends routing update messages at regular intervals and when network topology changes. When the FortiGate unit receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The FortiGate RIP table maintains the best route to a destination. After updating its routing table, the FortiGate unit begins transmitting routing updates to inform other network routers of the change. You can configure FortiGate RIP to control the timing of these updates.

RIP uses hop count as the routing metric to measure the distance between the source and destination network of a route. Each hop in the path of the route is added to the metric for the route. RIP prevents routing loops by limiting the number of hops allowed in a path to 15. This feature limits the maximum diameter of RIP network to 15 hops.

RIP uses a split horizon to prevent temporary routing loops caused by network topology changes. The premise of a split horizon is that it is never useful to send information about a route back in the direction from which it came. For example, Router 1 could tell Router 2 that it has a route for network A. Router 2 knows that it got this information from Router 1, so when Router 2 sends its updates to Router 1, Router 2 will not include the route to network A in its update. In this example, if Router 1 receives Router 2's information about the route to network A, Router 1 might try and use this route to get to network A rather than using its own.

RIP uses timers to regulate its performance. A routing update timer controls the time interval between routing updates. Usually this timer is set to 30 seconds. Each routing table entry has a route timeout. When the route timeout expires the route is marked as invalid. The invalid routes remain in the route table until the route flush timer expires.

RIP is a UDP-based protocol that sends and receives datagrams on UDP port 520. Unsolicited routing update messages have both the source and destination port equal to the RIP port. Update messages sent in response to a request are sent to the port from which the request came. Specific queries may be sent from ports other than the RIP port, but they must be directed to the RIP port on the target machine.

This chapter describes how to configure FortiGate RIP:

- [RIP settings](#)
- [Configuring RIP for FortiGate interfaces](#)
- [Adding RIP neighbors](#)
- [Adding RIP filters](#)

## RIP settings

Configure RIP settings to enable basic RIP functionality and metrics and to configure RIP timers.

- 1 Go to **System > RIP > Settings**.
- 2 Select Enable RIP Server to configure the FortiGate unit to be a RIP server.
- 3 Select Enable Advertise Default so that the FortiGate unit includes its default route in RIP routing table updates.
- 4 Select Enable Auto Summary to automatically summarize subnet routes into network-level routes.

If Enable Auto Summary is not selected, the FortiGate unit transmits sub-prefix routing information across classfull network boundaries.

- 5 Change the following RIP default settings to fine tune RIP performance.

RIP defaults are effective in most configurations. You should only have to change these settings to troubleshoot problems with your RIP configuration.

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default Metric</b> | Change the default metric that is applied to routes with incompatible metrics. The default metric assists in resolving how routes with incompatible metrics are redistributed. Whenever metrics do not convert, RIP uses the default metric to provide a reasonable substitute and allows the redistribution to proceed. The default setting of the default metric is 2.                                                                                                            |
| <b>Input Queue</b>    | Change the depth of the RIP input queue. The larger the numerical value, the larger the depth of the queue. Consider changing the input-queue depth if you have FortiGate unit sending at high speed to a low-speed router that might not be able to receive at the high speed. Configuring this command will help prevent the routing table from losing information. The range is 0 to 1024. The default input queue depth is 50. A queue size of 0 means there is no input queue. |
| <b>Output Delay</b>   | Change the output delay to add a delay in milliseconds between packets in a multiple-packet RIP update. A typical output delay is 8 to 50 milliseconds. Add an output delay if you are configuring RIP on a FortiGate unit that could be sending packets to a router that cannot receive the packets at the rate the FortiGate unit is sending them. The default output delay is 0 milliseconds.                                                                                    |

- 6 Change the following RIP timer settings to fine tune RIP performance.

RIP timer defaults are effective in most configurations. You should only have to change these timers to troubleshoot problems with your RIP configuration.

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Update</b>   | The time interval in seconds between sending routing table updates. The default is 30 seconds.                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Invalid</b>  | The time interval in seconds after which a route is declared invalid. Invalid should be at least three times the value of Update. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters holddown. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 180 seconds.                                                                                        |
| <b>Holddown</b> | The time interval in seconds during which routing information regarding better paths is suppressed. Holddown should be at least three times the value of Update. A route enters into a holddown state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable and is no longer used for forwarding packets. When holddown expires, the route can be flushed from the routing table. The default is 180 seconds. |
| <b>Flush</b>    | The amount of time in seconds that must pass before a route is removed from the routing table. The value for Flush should be greater than the value for Invalid. If the value for Flush is less than the value for Invalid, the proper holddown interval cannot elapse, which results in a new route being accepted before the holddown interval expires. The default is 240 seconds.                                                                                                             |

- 7 Select Apply to save your changes.

**Figure 1: Configuring RIP settings**

The screenshot shows a configuration window for RIP settings. At the top, there are three checked checkboxes: "Enable RIP Server", "Enable Advertise Default", and "Enable Auto Summary". Below these, there are three input fields: "Default Metric" with the value 2, "Input Queue" with the value 50, and "Output Delay" with the value 8. Under the heading "RIP Timer:", there are four input fields: "Update" (30 secs), "Invalid" (180 secs), "Holddown" (180 secs), and "Flush" (240 secs). At the bottom of the configuration area is a button labeled "Apply".

## Configuring RIP for FortiGate interfaces

You can create a unique RIP configuration for each FortiGate interface. This allows you to customize RIP for the network to which each interface is connected. For example:

- If you have a complex internal network containing devices that use the RIP2 protocol, you might want to configure RIP2 send and receive for the internal interface.
- If the external interface is connected to the Internet you may not want to enable RIP send for this interface so that the internal routes are not exposed to the Internet. However, you may want to configure RIP receive so that the FortiGate unit receives routes from your ISP.
- If the DMZ interface is connected to a small DMZ network you may not need to configure RIP for this interface.

### To configure RIP for FortiGate interfaces

- 1 Go to **System > RIP > Interface**.

On this page you can view a summary of the RIP settings for each FortiGate interface.

- 2 Select Modify  for the interface for which to configure RIP settings.

- 3 Configure the following RIP settings:

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RIP1 Send</b>      | This interface can send RIP1 routing broadcasts to routers on its network. The routing broadcasts are UDP packets with a destination port of 520.                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>RIP1 Receive</b>   | This interface can receive RIP1 routing broadcasts. The interface listens on port 520 for broadcast RIP1 messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>RIP2 Send</b>      | This interface can send RIP2 routing broadcasts to its network. The routing broadcasts are UDP packets with a destination port of 520.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>RIP2 Receive</b>   | This interface can receive RIP2 routing broadcasts. The interface listens on port 520 for broadcast RIP2 messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Split-Horizon</b>  | Configure split-horizon to prevent routing loops. By default, split horizon is enabled. This option should only be disabled if you are sure that routing loops cannot be created from this interface.                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Authentication</b> | Enable authentication for RIP2 packets sent and received by this interface. Authentication is only supported by RIP2. Do not select authentication if you are configuring the interface for RIP1.                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Password</b>       | Enter the password to be included in RIP2 requests. The password can be up to 16 characters long.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Mode</b>           | Defines how the FortiGate authenticates RIP2 packets. Select None, Clear, or MD5.<br>None means do not send the password.<br>Clear means send the password is plain text.<br>MD5 means use MD5 authentication.                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Metric</b>         | Changes the metric for routes sent by this interface. All routes sent from this interface will have this metric added to their current metric value. You can change interface metrics to give higher priorities to some interfaces. For example, if you have two interfaces that can be used to route packets to the same destination, if you set the metric of one interface higher than the other, the routes to the interface with the lower metric will seem to have a lower cost, so more traffic will use routes to the interface with the lower metric. The metric can be from 1 to 16. |



**Note:** MD5 authentication is used to verify the integrity of the routing message sent by the FortiGate unit. Using MD5 authentication, the password is added to the routing message and MD5 is applied to create the MD5 digest of the routing message. The password is replaced in the routing message with this MD5 digest and this message is broadcast. When a router receives the routing message, it replaces the MD5 digest with the password, computes the MD5 digest of this new message and then compares the result with the MD5 digest sent with the original message. If the two MD5 digests are identical, the receiver accepts the message. If they are not, the receiver rejects the message.

- 4 Select OK to save the RIP configuration for the selected interface.

**Figure 2: Example RIP configuration for an internal interface**

## Adding RIP neighbors

Add RIP neighbors to define a neighboring router with which to exchange routing information. Add neighbors on non-broadcast networks.

When you add neighbors, the FortiGate unit exchanges routing information with the neighbor router directly, instead of relying on broadcasting routes. This point-to-point exchange of routing information between the FortiGate unit and the routers added to the neighbor list is more secure and reduces network traffic. Adding neighbors is required to be able to exchange routes over non-broadcast networks.

When used in combination with the RIP filters, the FortiGate unit can be configured to exchange routing information with a subset of routers and access servers on a LAN.

### Adding RIP neighbors

- 1 Go to **System > RIP > Neighbor**.
- 2 Select New to add a RIP neighbor.

- 3 Add the IP address of a neighbor router that you want the FortiGate unit to exchange routing information with.
- 4 Select Enable Send RIP1 to send RIP1 messages to the neighbor.
- 5 Select Enable Send RIP2 to send RIP2 messages to the neighbor.
- 6 Select OK to add the RIP neighbor to the list.

## Adding RIP filters

Use RIP filters to control the routing information received by the FortiGate unit and sent by the FortiGate unit. You can create filters for two purposes:

**Neighbors filter** For filtering routes received from neighboring routers. When the FortiGate unit receives routes from a neighboring router, the neighbors filter defines what routes received from the neighbor will be stored in the FortiGate routing table and what routes will be discarded.

**Routes filter** For filtering routes before a routing table update is sent to neighboring routers. Before the FortiGate unit sends routes to neighboring routers, the routes filter defines what routes can be sent and what routes cannot be sent.

A RIP filter consists of the IP address and netmask of a route, the action the filter should perform for this route (allow or deny), and the interface on which this filter entry should be applied. Routes that do not match a route added to a RIP filter are allowed.

A single RIP filter contains instructions for allowing or denying a single route. You can add multiple RIP filter entries under the same RIP filter name to create a RIP filter list. Using a RIP filter list you can filter multiple routes.

After creating RIP filters and filter lists you can configure the neighbors filter or routes filter by selecting a filter or filter list for each of these filter types. If you do not select a RIP filter for neighbors or routes, no filtering is applied. You can add a total of four RIP filters or RIP filter lists, but you can only have one active neighbors filter and one active routes filter.

This section describes:

- [Adding a single RIP filter](#)
- [Adding a RIP filter list](#)
- [Adding a neighbors filter](#)
- [Adding a routes filter](#)

### Adding a single RIP filter

Add a single RIP filter to filter a single route. You can apply a single RIP filter to the neighbors or routes filter. You can add a total of four RIP filters or RIP Filter lists.

If you want to filter multiple routes, use a RIP filter list. See [“Adding a RIP filter list” on page 127](#).

- 1 Go to **System > RIP > Filter**.
- 2 Select New to add a RIP filter.
- 3 Configure the RIP filter.

|                     |                                                                                                                                                                                                                                               |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Filter Name</b>  | Enter a name for the RIP filter. Each RIP filter and RIP filter list must have unique name. The name can be 15 characters long and can contain upper and lower case letters, numbers, and special characters. The name cannot contain spaces. |
| <b>Blank Filter</b> | Used for Filter lists. See <a href="#">“Adding a RIP filter list” on page 127</a> .                                                                                                                                                           |
| <b>IP</b>           | Add the IP address of the route.                                                                                                                                                                                                              |
| <b>Mask</b>         | Add the netmask of the route.                                                                                                                                                                                                                 |
| <b>Action</b>       | Select Allow so that the filter permits this route to be communicated. Select Deny to stop this route from being communicated.                                                                                                                |
| <b>Interface</b>    | Select the interface on which to apply this RIP filter.                                                                                                                                                                                       |

- 4 Select OK to save the RIP filter.

## Adding a RIP filter list

Add a RIP filter list to filter multiple routes. A RIP filter list consists of a RIP filter name and a series of route prefixes. You can add a total of four RIP filters or RIP Filter lists.

When a RIP filter list is added to the neighbors or routes filter, all of the routes in the RIP filter list are filtered.

- 1 Go to **System > RIP > Filter**.
- 2 Select New to add a RIP filter.
- 3 Configure the RIP filter list name.

|                     |                                                                                                                                                                                                                                                    |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Filter Name</b>  | Enter a name for the RIP filter list. Each RIP filter and RIP filter list must have unique name. The name can be 15 characters long and can contain upper and lower case letters, numbers, and special characters. The name cannot contain spaces. |
| <b>Blank Filter</b> | Optionally select blank filter to start the RIP filter list with a blank x. After adding the blank filter you can add routes to the RIP filter list.                                                                                               |

- 4 Select OK to save the RIP filter list.
- 5 For the RIP filter list name, select  Add Prefix to add a route prefix to the filter list.
- 6 Configure the route prefix.

|                  |                                                                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>IP</b>        | Add the IP address of the route.                                                                                               |
| <b>Mask</b>      | Add the netmask of the route.                                                                                                  |
| <b>Action</b>    | Select Allow so that the filter permits this route to be communicated. Select Deny to stop this route from being communicated. |
| <b>Interface</b> | Select the interface on which to apply this RIP filter.                                                                        |

- 7 Select OK to add the route prefix to the filter list.
- 8 Repeat steps 5 to 7 to add route prefixes to the filter list.

## Adding a neighbors filter

You can select a single RIP filter or a RIP filter list to be the neighbors filter.

- 1 Go to **System > RIP > Filter**.
- 2 Add RIP filters and RIP filter lists as required.
- 3 For Neighbors Filter, select the name of the RIP filter or RIP filter list to become the neighbors filter.
- 4 Select Apply.  
Routes received from neighbors are filtered using the selected RIP filter or RIP filter list.

## Adding a routes filter

You can select a single RIP filter or a RIP filter list to be the routes filter.

- 1 Go to **System > RIP > Filter**.
- 2 Add RIP filters and RIP filter lists as required.
- 3 For Routes Filter, select the name of the RIP filter or RIP filter list to become the routes filter.
- 4 Select Apply.  
Routes sent by the FortiGate unit are filtered using the selected RIP filter or RIP filter list.

**Figure 3: Example RIP Filter configuration**

Neighbors Filter: Filter\_1
Routes Filter: Filter\_List\_2
Apply

| filter        | IP       | Mask          | Action | Interface | modify                                       |
|---------------|----------|---------------|--------|-----------|----------------------------------------------|
| Filter_1      | 2.3.4.5  | 255.255.255.0 | allow  | internal  | <span style="font-size: 0.8em;">⊞ ⊞ ⊞</span> |
| Filter_List_1 | 2.3.4.5  | 255.255.255.0 | deny   | internal  | <span style="font-size: 0.8em;">⊞ ⊞</span>   |
|               | 2.6.5.4  | 255.255.255.0 | allow  | internal  | <span style="font-size: 0.8em;">⊞</span>     |
|               | 5.3.4.6  | 255.255.255.0 | deny   | internal  | <span style="font-size: 0.8em;">⊞</span>     |
|               | 2.4.5.67 | 255.255.255.0 | deny   | external  | <span style="font-size: 0.8em;">⊞ ⊞</span>   |
| Filter_2      | 3.2.5.6  | 255.255.255.0 | allow  | internal  | <span style="font-size: 0.8em;">⊞ ⊞ ⊞</span> |
| Filter_List_2 | 3.2.4.5  | 255.255.255.0 | allow  | internal  | <span style="font-size: 0.8em;">⊞ ⊞</span>   |
|               | 5.34.8.9 | 255.255.255.0 | deny   | internal  | <span style="font-size: 0.8em;">⊞ ⊞</span>   |

New

# System configuration

Go to **System > Config** to make any of the following changes to the FortiGate system configuration:

- [Setting system date and time](#)
- [Changing web-based manager options](#)
- [Adding and editing administrator accounts](#)
- [Configuring SNMP](#)
- [Customizing replacement messages](#)

## Setting system date and time

For effective scheduling and logging, the FortiGate system time should be accurate. You can either manually set the FortiGate system time or you can configure the FortiGate unit to automatically keep its system time correct by synchronizing with a Network Time Protocol (NTP) server.

For more information on NTP and to find the IP address of an NTP server that you can use, see <http://www.ntp.org>.

### To set the date and time

- 1 Go to **System > Config > Time**.
- 2 Select Refresh to display the current FortiGate system date and time.
- 3 Select your Time Zone from the list.
- 4 Select Automatically adjust clock for daylight saving changes if you want the FortiGate system clock to be adjusted automatically when your time zone changes to daylight saving time.
- 5 Select Set Time and set the FortiGate system date and time to the correct date and time if required.
- 6 Select Synchronize with NTP Server to configure the FortiGate unit to use NTP to automatically set the system time and date.

You can go to [www.ntp.org](http://www.ntp.org) for information about the network time protocol (NTP) and to select a public NTP server in your region.

- 7 Enter the IP address or domain name of the NTP server that the FortiGate unit uses to set its time and date.

- 8 Specify how often the FortiGate unit should synchronize its time with the NTP server. A typical Syn Interval would be 1440 minutes for the FortiGate unit to synchronize its time once a day.
- 9 Select Apply.

**Figure 1: Example date and time setting**

**System Time** Tue Jun 24 07:18:53 2003 **Refresh**

**Time Zone** (GMT-8:00)Pacific Time(US&Canada) ▼

☐ Automatically adjust clock for daylight saving changes

☒ **Set Time** Hour 7 Minute 18 Second 53  
Month Jun Day 24 Year 2003

☐ **Synchronize with NTP Server**

Server 132.246.168.148

Syn Interval 60 (mins)

**Apply**

## Changing web-based manager options

On the System > Config > Options page, you can:

- Set the system idle timeout.
- Set the authentication timeout.
- Select the language for the web-base manager.
- Modify the dead gateway detection settings.

### To set the system idle timeout

- 1 For Idle Timeout, type a number in minutes.
- 2 Select Apply.

Idle Timeout controls the amount of inactive time that the web-based manager waits before requiring the administrator to log in again.

The default idle time out is 5 minutes. The maximum idle time out is 480 minutes (8 hours).

### To set the Auth timeout

- 1 For Auth Timeout, type a number in minutes.
- 2 Select Apply.

Auth Timeout controls the amount of inactive time that the firewall waits before requiring users to authenticate again. For more information, see [“Users and authentication” on page 173](#).

The default Auth Timeout is 15 minutes. The maximum Auth Timeout is 480 minutes (8 hours).

### To select a language for the web-based manager

- 1 From the Languages list, select a language that the web-based manager uses.
- 2 Select Apply.

You can choose from English, Simplified Chinese, Japanese, Korean, or Traditional Chinese.



**Note:** When the web-based manager language is set to use Simplified Chinese, Japanese, Korean, or Traditional Chinese, you can change to English by selecting the English button on the upper right of the web-based manager.

### To modify the Dead Gateway Detection settings

Modify dead gateway detection to control how the FortiGate unit confirms connectivity with a ping server added to an interface configuration. To add a ping server to an interface, see [“Adding a ping server to an interface” on page 111](#).

- 1 For Detection Interval, type a number in seconds to specify how often the FortiGate unit tests the connection to the ping target.
- 2 For Fail-over Detection, type a number of times that the connection test fails before the FortiGate unit assumes that the gateway is no longer functioning.
- 3 Select Apply.

## Adding and editing administrator accounts

When the FortiGate unit is initially installed, it is configured with a single administrator account with the user name admin. From this administrator account, you can add and edit administrator accounts. You can also control the access level of each of these administrator accounts and, optionally, control the IP address from which the administrator can connect to the FortiGate unit.

There are three administration account access levels:

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>admin</b>            | Has all permissions. Can view, add, edit, and delete administrator accounts. Can view and change the FortiGate configuration. The admin user is the only user who can go to <b>System &gt; Status</b> and manually update firmware, update the antivirus definitions, update the attack definitions, download or upload system settings, restore the FortiGate unit to factory defaults, restart the FortiGate unit, and shut down the FortiGate unit. There is only one admin user. |
| <b>Read &amp; Write</b> | Can view and change the FortiGate configuration. Can view but cannot add, edit, or delete administrator accounts. Can change own administrator account password. Cannot make changes to system settings from the <b>System &gt; Status</b> page.                                                                                                                                                                                                                                     |
| <b>Read Only</b>        | Can view the FortiGate configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                |

### Adding new administrator accounts

From the admin account, use the following procedure to add new administrator accounts and control their permission levels:

- 1 Go to **System > Config > Admin**.
- 2 Select New to add an administrator account.
- 3 Type a login name for the administrator account.

The login name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.

- 4 Type and confirm a password for the administrator account.

For improved security, the password should be at least 6 characters long. The password can contain any characters except spaces.

- 5 Optionally type a Trusted Host IP address and netmask for the location from which the administrator can log into the web-based manager.

If you want the administrator to be able to access the FortiGate unit from any address, set the trusted host to 0.0.0.0 and the netmask to 0.0.0.0.

To limit the administrator to only be able to access the FortiGate unit from a specific network, set the trusted host to the address of the network and set the netmask to the netmask for the network. For example, to limit an administrator to accessing the FortiGate unit from your internal network, set the trusted host to the address of your internal network (for example, 192.168.1.0) and set the netmask to 255.255.255.0.

- 6 Set the Permission level for the administrator.
- 7 Select OK to add the administrator account.

## Editing administrator accounts

The admin account user can change individual administrator account passwords, configure the IP addresses from which administrators can access the web-based manager, and change the administrator permission levels.

Administrator account users with Read & Write access can change their own administrator passwords.

### To edit an administrator account

- 1 Go to **System > Config > Admin**.
- 2 To change an administrator account password, select Change Password .
- 3 Type the Old Password.
- 4 Type a New Password and Confirm the new password.  
For improved security, the password should be at least 6 characters long. The password can contain any characters except spaces. If you enter a password that is less than 6 characters long, the system displays a warning message but still accepts the password.
- 5 Select OK.
- 6 To edit the settings of an administrator account, select Edit .
- 7 Optionally type a Trusted Host IP address and netmask for the location from which the administrator can log into the web-based manager.  
If you want the administrator to be able to access the FortiGate unit from any address, set the trusted host to 0.0.0.0 and the netmask to 255.255.255.255.  
To limit the administrator to only be able to access the FortiGate unit from a specific network, set the trusted host to the address of the network and set the netmask to the netmask for the network. For example, to limit an administrator to accessing the FortiGate unit from your internal network, set the trusted host to the address of your internal network (for example, 192.168.1.0) and set the netmask to 255.255.255.0.
- 8 Change the administrator's permission level as required.
- 9 Select OK.
- 10 To delete an administrator account, choose the account to delete and select Delete .

## Configuring SNMP

Configure the FortiGate SNMP agent to report system information and send traps to SNMP managers. The FortiGate SNMP agent supports SNMP v1 and v2c. RFC support includes RFC 1213 and RFC 2665. The FortiGate SNMP implementation is read-only. SNMP v1 and v2c compliant SNMP manager have read-only access to FortiGate system information and can receive FortiGate traps. To monitor FortiGate system information and receive FortiGate traps you must compile the Fortinet proprietary MIBs and the standard MIBs into the SNMP manager.

This section describes:

- [Configuring the FortiGate unit for SNMP monitoring](#)
- [Configuring FortiGate SNMP support](#)
- [FortiGate MIBs](#)
- [FortiGate traps](#)

### Configuring the FortiGate unit for SNMP monitoring

Before a remote SNMP manager can connect to the FortiGate agent, you must configure one or more FortiGate interfaces to accept SNMP connections. For information about how to do this, see [“Controlling management access to an interface” on page 111](#) and related interface configuration sections.

### Configuring FortiGate SNMP support

- 1 Go to **System > Config > SNMP v1/v2c**.
- 2 Select **Enable SNMP**.
- 3 Configure SNMP settings:

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System Name</b>         | Automatically set to the FortiGate host name. To change the System Name, see <a href="#">“Changing the FortiGate host name” on page 70</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>System Location</b>     | Describe the physical location of the FortiGate unit. The system location description can be up to 31 characters long and can contain spaces, numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. The \ < > [ ] ` \$ % & characters are not allowed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Contact Information</b> | Add the contact information for the person responsible for this FortiGate unit. The contact information can be up to 31 characters long and can contain spaces, numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. The \ < > [ ] ` \$ % & characters are not allowed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Get Community</b>       | <p>Also called read community, get community is a password to identify SNMP get requests sent to the FortiGate unit. When an SNMP manager sends a get request to the FortiGate unit, it must include the correct get community string.</p> <p>The default get community string is “public”. Change the default get community string to keep intruders from using get requests to retrieve information about your network configuration. The get community string must be used in your SNMP manager to enable it to access FortiGate SNMP information.</p> <p>The get community string can be up to 31 characters long and can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Spaces and the \ &lt; &gt; [ ] ` \$ % &amp; characters are not allowed.</p> |

- Trap Community** The trap community string functions like a password that is sent with SNMP traps.  
The default trap community string is "public". Change the trap community string to the one accepted by your trap receivers.  
The trap community string can be up to 31 characters long and can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Spaces and the \ < > [ ] ` \$ % & characters are not allowed.
- Trap Receiver IP Addresses** Type the IP addresses of up to three trap receivers on your network that are configured to receive traps from your FortiGate unit. Traps are only sent to the configured addresses.

4 Select Apply.

Figure 2: Sample SNMP configuration

The image shows a sample SNMP configuration form. It includes the following fields and values:

- Enable SNMP:** ☒
- System Name:** Main\_Office\_Firewall
- System Location:** Server room first floor
- Contact Information:** ext 3345
- Get Community:** our\_get\_com
- Trap Community:** trap\_com
- First Trap Receiver IP Address:** 192.33.44.55
- Second Trap Receiver IP Address:** 143.44.52.78
- Third Trap Receiver IP Address:** (empty field)
- Apply** button

## FortiGate MIBs

The FortiGate SNMP agent supports FortiGate proprietary MIBs as well as standard RFC 1213 and RFC 2665 MIBs. The FortiGate MIBs are listed in [Table 1](#). You can obtain these MIB files from Fortinet technical support. To be able to communicate with the SNMP agent, all of these MIBs must be compiled into your SNMP manager.

Your SNMP manager may already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIBs to this database. If the standard MIBs used by the Fortinet SNMP agent are already compiled into your SNMP manager you will not have to re-compile them.

Table 1: FortiGate MIBs

| MIB file name        | Description                                                                                                                                                                                                                    |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>EtherLike.mib</b> | The Ethernet-like MIB is a standard MIB based on RFC 2665. This MIB includes information used for managing ethernet interfaces.                                                                                                |
| <b>FN-TRAP.mib</b>   | The Fortinet trap MIB is a proprietary MIB that is required for your SNMP manager to receive traps from the FortiGate SNMP agent. For more information on FortiGate traps, see <a href="#">"FortiGate traps" on page 136</a> . |

**Table 1: FortiGate MIBs**

| MIB file name       | Description                                                                                                                                                                                 |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FORTINET.mib</b> | The Fortinet MIB is a proprietary MIB that includes detailed FortiGate system configuration information. Add this MIB to your SNMP manager to monitor all FortiGate configuration settings. |
| <b>RFC1213.mib</b>  | The RFC 1213 MIB is the standard MIB-II MIB that describes network management protocols for TCP/IP networks.                                                                                |

## FortiGate traps

The FortiGate agent can send traps to up to three SNMP trap receivers on your network that are configured to receive traps from the FortiGate unit. For these SNMP managers to receive traps, you must load and compile the Fortinet trap MIB onto the SNMP manager. The FortiGate agent sends the traps listed in [Table 2](#).

**Table 2: FortiGate traps**

| Trap message                                                                                           | Description                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The <interface_name> Interface IP is changed to <new_IP> (Fortigate Serial No.: <FortiGate_serial_no>) | The IP address of an interface of a FortiGate unit has changed. The trap message includes the name of the interface for which the IP address changed, the new IP address of the interface, and the serial number of the FortiGate unit. This trap can be used to track interface IP address changes for interfaces configured with dynamic IP addresses set using DHCP or PPPoE. |
| System Down                                                                                            | The FortiGate unit is shutting down.                                                                                                                                                                                                                                                                                                                                             |
| Agent Down                                                                                             | An administrator has disabled the SNMP agent. This trap is also sent when the agent stops before a system shutdown.                                                                                                                                                                                                                                                              |
| Cold Start                                                                                             | The FortiGate unit starts or restarts. An administrator enables the SNMP agent or changes FortiGate SNMP settings. This trap is sent when the agent starts during system startup.                                                                                                                                                                                                |
| Authentication failure                                                                                 | An SNMP manager community string does not match the FortiGate get community string                                                                                                                                                                                                                                                                                               |

## Customizing replacement messages

Replacement messages are added to content passing through the firewall to replace:

- Files or other content removed from email messages by the antivirus system
- Files or other content removed from HTTP downloads by the antivirus system or web filtering
- Files removed from FTP downloads by the antivirus system

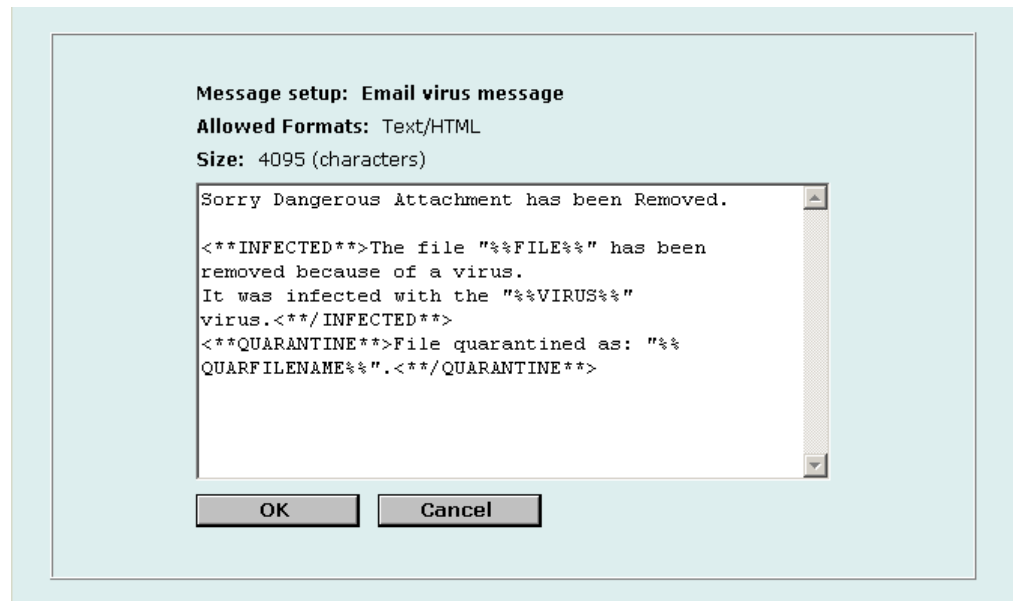
You can edit replacement messages to control the content of these messages when they are received by a user.

You can also edit the content added to alert email messages to control the information that appears in alert emails for virus incidents, NIDS events, critical system events, and disk full events.

This section describes:

- [Customizing replacement messages](#)
- [Customizing alert emails](#)

**Figure 3: Sample replacement message**



## Customizing replacement messages

Each of the replacement messages in the replacement message list is created by combining replacement message sections. You can use these sections as building blocks to create your own replacement messages.

You can edit any of the replacement messages in the replacement message list and add and edit the replacement message sections as required.

- 1 Go to **System > Config > Replacement Messages**.
- 2 For the replacement message you want to customize, select Modify .
- 3 In the Message setup dialog box, edit the content of the message.  
[Table 3](#) lists the replacement message sections that can be added to replacement messages and describes the tags that can appear in each section. In addition to the allowed tags you can add any text. Also for mail and HTTP messages you can add HTML code.
- 4 Select OK to save the changes.

**Table 3: Replacement message sections**

|                      |                                        |                                        |
|----------------------|----------------------------------------|----------------------------------------|
| <b>File blocking</b> | Used for file blocking (all services). |                                        |
| <b>Section Start</b> | < **BLOCKED** >                        |                                        |
| <b>Allowed Tags</b>  | %%FILE%%                               | The name of the file that was blocked. |
|                      | %%URL%%                                | The URL of the blocked web page.       |
| <b>Section End</b>   | < **/BLOCKED** >                       |                                        |

**Table 3: Replacement message sections**

|                      |                                         |                                           |
|----------------------|-----------------------------------------|-------------------------------------------|
| <b>Scanning</b>      | Used for virus scanning (all services). |                                           |
| <b>Section Start</b> | < **INFECTED** >                        |                                           |
| <b>Allowed Tags</b>  | %%FILE%%                                | The name of the file that was infected.   |
|                      | %%VIRUS%%                               | The name of the virus infecting the file. |
|                      | %%URL%%                                 | The URL of the blocked web page or file.  |
| <b>Section End</b>   | < **/BLOCKED** >                        |                                           |

|                      |                                                                                                      |                                            |
|----------------------|------------------------------------------------------------------------------------------------------|--------------------------------------------|
| <b>Quarantine</b>    | Used when quarantine is enabled (permitted for all scan services and block services for email only). |                                            |
| <b>Section Start</b> | < **QUARANTINE** >                                                                                   |                                            |
| <b>Allowed Tag</b>   | %%QUARFILE<br>NAME%%                                                                                 | The name of the file that was quarantined. |
| <b>Section End</b>   | < **/QUARANTINE** >                                                                                  |                                            |

## Customizing alert emails

Customize alert emails to control the content displayed in alert email messages sent to system administrators.

- 1 Go to **System > Config > Replacement Messages**.
- 2 For the alert email message you want to customize, select Modify .
- 3 In the Message setup dialog box, edit the text of the message.  
[Table 4](#) lists the replacement message sections that can be added to alert email messages and describes the tags that can appear in each section. In addition to the allowed tags you can add any text and HTML code.
- 4 Select OK to save the changes.

**Table 4: Alert email message sections**

|                      |                                          |                          |
|----------------------|------------------------------------------|--------------------------|
| <b>NIDS event</b>    | Used for NIDS event alert email messages |                          |
| <b>Section Start</b> | < **NIDS_EVENT** >                       |                          |
| <b>Allowed Tags</b>  | %%NIDS_EVENT%%                           | The NIDS attack message. |
| <b>Section End</b>   | < **/NIDS_EVENT** >                      |                          |

|                      |                                     |                                                                                                                                                                                                                   |
|----------------------|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Virus alert</b>   | Used for virus alert email messages |                                                                                                                                                                                                                   |
| <b>Section Start</b> | < **VIRUS_ALERT** >                 |                                                                                                                                                                                                                   |
| <b>Allowed Tags</b>  | %%VIRUS%%                           | The name of the virus.                                                                                                                                                                                            |
|                      | %%PROTOCOL%%                        | The service for which the virus was detected.                                                                                                                                                                     |
|                      | %%SOURCE_IP%%                       | The IP address from which the virus was received. For email this is the IP address of the email server that sent the email containing the virus. For HTTP this is the IP address of web page that sent the virus. |
|                      | %%DEST_IP%%                         | The IP address of the computer that would have received the virus. For POP3 this is the IP address of the user's computer that attempted to download the email containing the virus.                              |

**Table 4: Alert email message sections**

|  |                |                                                                                         |
|--|----------------|-----------------------------------------------------------------------------------------|
|  | %%EMAIL_FROM%% | The email address of the sender of the message in which the virus was found.            |
|  | %%EMAIL_TO%%   | The email address of the intended receiver of the message in which the virus was found. |

|                      |                                          |                                                                                                                                                                                                                                      |
|----------------------|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Block alert          | Used for file block alert email messages |                                                                                                                                                                                                                                      |
| <b>Section Start</b> | <**BLOCK_ALERT**>                        |                                                                                                                                                                                                                                      |
| <b>Allowed Tags</b>  | %%FILE%%                                 | The name of the file that was blocked.                                                                                                                                                                                               |
|                      | %%PROTOCOL%%                             | The service for which the file was blocked.                                                                                                                                                                                          |
|                      | %%SOURCE_IP%%                            | The IP address from which the block file was received. For email this is the IP address of the email server that sent the email containing the blocked file. For HTTP this is the IP address of web page that sent the blocked file. |
|                      | %%DEST_IP%%                              | The IP address of the computer that would have received the blocked file. For email this is the IP address of the user's computer that attempted to download the message from which the file were removed.                           |
|                      | %%EMAIL_FROM%%                           | The email address of the sender of the message from which the file was removed.                                                                                                                                                      |
|                      | %%EMAIL_TO%%                             | The email address of the intended receiver of the message from which the file was removed.                                                                                                                                           |

|                      |                                                |                                     |
|----------------------|------------------------------------------------|-------------------------------------|
| Critical event       | Used for critical firewall event alert emails. |                                     |
| <b>Section Start</b> | <**CRITICAL_EVENT**>                           |                                     |
| <b>Allowed Tags</b>  | %%CRITICAL_EVENT%%<br>%%                       | The firewall critical event message |
| <b>Section End</b>   | <**/CRITICAL_EVENT**>                          |                                     |



# Firewall configuration

Firewall policies control all traffic passing through the FortiGate unit. Firewall policies are instructions used by the FortiGate unit to decide what to do with a connection request. When the firewall receives a connection request in the form of a packet, it analyzes the packet to extract its source address, destination address, and service (port number).

For the packet to be connected through the FortiGate unit, a firewall policy must have been added that matches the packet's source address, destination address, and service. The policy directs the firewall action on the packet. The action can be to allow the connection, deny the connection, require authentication before the connection is allowed, or process the packet as an IPsec VPN packet. You can also add schedules to policies so that the firewall can process connections differently depending on the time of day or the day of the week, month, or year.

Each policy can be individually configured to route connections or to apply network address translation (NAT) to translate source and destination IP addresses and ports. You can add IP pools to use dynamic NAT when the firewall translates source addresses. You can use policies to configure port address translation (PAT) through the FortiGate.

Content profiles can be added to policies to apply antivirus protection, web filtering, and email filtering to web, file transfer, and email services. You can create content profiles that perform one or any combination of the following actions:

- Apply antivirus protection to HTTP, FTP, SMTP, IMAP, or POP3 services.
- Apply web filtering to HTTP services.
- Apply email filtering to IMAP and POP3 services.

You can also add logging to a firewall policy so that the FortiGate unit logs all connections that use this policy.

This chapter describes:

- [Default firewall configuration](#)
- [Adding firewall policies](#)
- [Configuring policy lists](#)
- [Addresses](#)
- [Services](#)
- [Schedules](#)
- [Virtual IPs](#)
- [IP pools](#)
- [IP/MAC binding](#)
- [Content profiles](#)

## Default firewall configuration

By default, the users on your internal network can connect through the FortiGate unit to the Internet. The firewall blocks all other connections. The firewall is configured with a default policy that matches any connection request received from the internal network and instructs the firewall to forward the connection to the Internet.

**Figure 4: Default firewall policy**

| # | ID | Source       | Dest         | Schedule | Service | Action | Enable                              | Config                                                                                                                                                                                                                                                                                                                                          |
|---|----|--------------|--------------|----------|---------|--------|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | 1  | Internal_All | External_All | Always   | ANY     | ACCEPT | <input checked="" type="checkbox"/> |     |

- [Addresses](#)
- [Services](#)
- [Schedules](#)
- [Content profiles](#)

### Addresses

Add policies to control connections between FortiGate interfaces and between the networks connected to these interfaces. To add policies between interfaces, the interfaces must include addresses. By default the FortiGate unit is configured with the following firewall addresses:

- Internal\_All, added to the internal interface, this address matches all addresses on the internal network.
- External\_All, added to the external interface, this address matches all addresses on the external network.
- DMZ\_All, added to the DMZ interface, this address matches all addresses on the DMZ network.

The firewall uses these addresses to match the source and destination addresses of packets received by the firewall. The default policy matches all connections from the internal network because it includes the Internal\_All address. The default policy also matches all connections to the external network because it includes the External\_All address.

You can add more addresses to each interface to improve the control you have over connections through the firewall. For more information about firewall addresses, see [“Addresses” on page 150](#).

You can also add firewall policies that perform network address translation (NAT). To use NAT to translate destination addresses, you must add virtual IPs. Virtual IPs map addresses on one network to a translated address on another network. For more information about Virtual IPs, see [“Virtual IPs” on page 160](#).

## Services

Policies can also control connections based on the service or destination port number of packets. The default policy accepts connections to using any service or destination port number. The firewall is configured with over 40 predefined services. You can add these services to a policy for more control over the services that can be used by connections through the firewall. You can also add user-defined services. For more information about services, see [“Services” on page 153](#).

## Schedules

Policies can also control connections based on the time of day or day of the week when the firewall receives the connection. The default policy accepts connections at any time. The firewall is configured with one schedule that accepts connections at any time. You can add more schedules to control when policies are active. For more information about schedules, see [“Schedules” on page 157](#).

## Content profiles

Content profiles can be added to policies to apply antivirus protection, web filtering, and email filtering to web, file transfer, and email services. The FortiGate unit includes the following default content profiles:

- Strict: to apply maximum content protection to HTTP, FTP, IMAP, POP3, and SMTP content traffic.
- Scan: to apply antivirus scanning to HTTP, FTP, IMAP, POP3, and SMTP content traffic.
- Web: to apply antivirus scanning and Web content blocking to HTTP content traffic.
- Unfiltered: to allow oversized files to pass through the FortiGate unit without scanned for viruses.

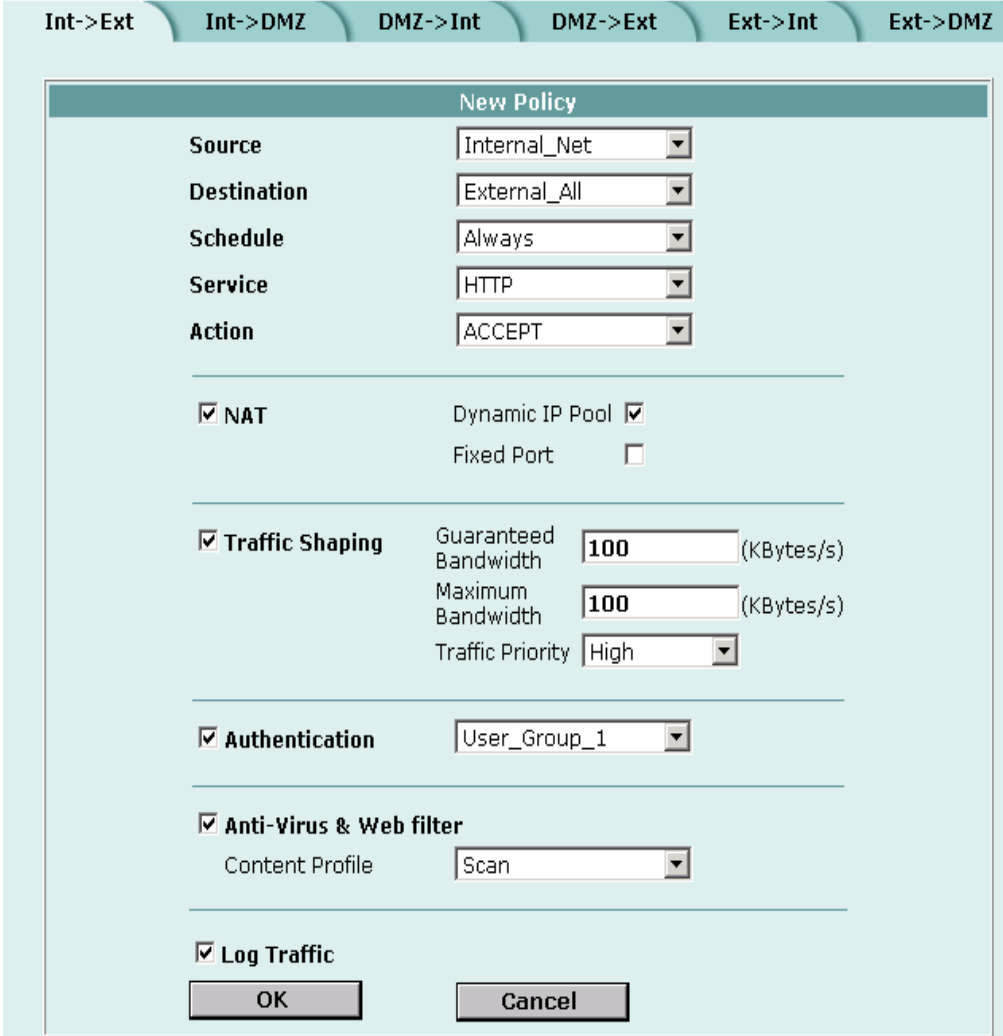
For more information about content profiles, see [“Content profiles” on page 169](#).

## Adding firewall policies

Add Firewall policies to control connections and traffic between FortiGate interfaces.

- 1 Go to **Firewall > Policy**.
- 2 Select the policy list to which you want to add the policy.
- 3 Select New to add a new policy.  
You can also select Insert Policy before  on a policy in the list to add the new policy above a specific policy.
- 4 Configure the policy:  
See [“Firewall policy options” on page 145](#) for information about policy options.
- 5 Select OK to add the policy.
- 6 Arrange policies in the policy list so that they have the results that you expect.  
Arranging policies in a policy list is described in [“Configuring policy lists” on page 149](#).

**Figure 5: Adding a NAT/Route policy**



**New Policy**

Int->Ext   Int->DMZ   DMZ->Int   DMZ->Ext   Ext->Int   Ext->DMZ

Source: Internal\_Net

Destination: External\_All

Schedule: Always

Service: HTTP

Action: ACCEPT

---

☒ NAT      Dynamic IP Pool ☒  
Fixed Port ☐

---

☒ Traffic Shaping      Guaranteed Bandwidth: 100 (KBytes/s)  
Maximum Bandwidth: 100 (KBytes/s)  
Traffic Priority: High

---

☒ Authentication      User\_Group\_1

---

☒ Anti-Virus & Web filter  
Content Profile: Scan

---

☒ Log Traffic

OK      Cancel

## Firewall policy options

This section describes the options that you can add to firewall policies.

### Source

Select an address or address group that matches the source address of the packet. Before you can add this address to a policy, you must add it to the source interface. To add an address, see [“Addresses” on page 150](#).

### Destination

Select an address or address group that matches the destination address of the packet. Before you can add this address to a policy, you must add it to the destination interface. To add an address, see [“Addresses” on page 150](#).

For NAT/Route mode policies where the address on the destination network is hidden from the source network using NAT, the destination can also be a virtual IP that maps the destination address of the packet to a hidden destination address. See [“Virtual IPs” on page 160](#).

### Schedule

Select a schedule that controls when the policy is available to be matched with connections. See [“Schedules” on page 157](#).

### Service

Select a service that matches the service (port number) of the packet. You can select from a wide range of predefined services or add custom services and service groups. See [“Services” on page 153](#).

### Action

Select how the firewall should respond when the policy matches a connection attempt.

|                |                                                                                                                                                                                                                                                                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ACCEPT</b>  | Accept the connection. If you select ACCEPT, you can also configure NAT and Authentication for the policy.                                                                                                                                                                                                                                |
| <b>DENY</b>    | Deny the connection. The only other policy option that you can configure is log traffic, to log the connections denied by this policy.                                                                                                                                                                                                    |
| <b>ENCRYPT</b> | Make this policy an IPsec VPN policy. If you select ENCRYPT, you can select an AutoIKE key or Manual Key VPN tunnel for the policy and configure other IPsec settings. You cannot add authentication to an ENCRYPT policy. ENCRYPT is not available in Transparent mode. See <a href="#">“Configuring encrypt policies” on page 196</a> . |

### NAT

Configure the policy for NAT. NAT translates the source address and the source port of packets accepted by the policy. If you select NAT, you can also select Dynamic IP Pool and Fixed Port. NAT is not available in Transparent mode.

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Dynamic IP Pool</b> | You cannot select Dynamic IP Pool for Int->Ext or DMZ->Ext policies if the external interface is configured using DHCP or PPPoE.<br>Select Dynamic IP Pool to translate the source address to an address randomly selected from an IP pool added to the destination interface of the policy. To add IP pools, see <a href="#">“IP pools” on page 164</a> .                                                                                 |
| <b>Fixed Port</b>      | Select Fixed Port to prevent NAT from translating the source port. Some applications do not function correctly if the source port is changed. If you select Fixed Port, you must also select Dynamic IP Pool and add a dynamic IP pool address range to the destination interface of the policy. If you do not select Dynamic IP Pool, a policy with Fixed Port selected can only allow one connection at a time for this port or service. |

## VPN Tunnel

Select a VPN tunnel for an ENCRYPT policy. You can select an AutoIKE key or Manual Key tunnel. VPN Tunnel is not available in Transparent mode.

|                       |                                                                                                               |
|-----------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Allow inbound</b>  | Select Allow inbound so that users behind the remote VPN gateway can connect to the source address.           |
| <b>Allow outbound</b> | Select Allow outbound so that users can connect to the destination address behind the remote VPN gateway.     |
| <b>Inbound NAT</b>    | Select Inbound NAT to translate the source address of incoming packets to the FortiGate internal IP address.  |
| <b>Outbound NAT</b>   | Select Outbound NAT to translate the source address of outgoing packets to the FortiGate external IP address. |

## Traffic Shaping

Traffic Shaping controls the bandwidth available to and sets the priority of the traffic processed by the policy. Traffic Shaping makes it possible to control which policies have the highest priority when large amounts of data are moving through the FortiGate device. For example, the policy for the corporate web server might be given higher priority than the policies for most employees' computers. An employee who needs unusually high-speed Internet access could have a special outgoing policy set up with higher bandwidth.

If you set both guaranteed bandwidth and maximum bandwidth to 0 the policy does not allow any traffic.

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Guaranteed Bandwidth</b> | You can use traffic shaping to guarantee the amount of bandwidth available through the firewall for a policy. Guarantee bandwidth (in Kbytes) to make sure that there is enough bandwidth available for a high-priority service.                                                                                                                                                                                                                                                    |
| <b>Maximum Bandwidth</b>    | You can also use traffic shaping to limit the amount of bandwidth available through the firewall for a policy. Limit bandwidth to keep less important services from using bandwidth needed for more important services.                                                                                                                                                                                                                                                             |
| <b>Traffic Priority</b>     | Select High, Medium, or Low. Select Traffic Priority so that the FortiGate unit manages the relative priorities of different types of traffic. For example, a policy for connecting to a secure web server needed to support e-commerce traffic should be assigned a high traffic priority. Less important services should be assigned a low priority. The firewall provides bandwidth to low-priority connections only when bandwidth is not needed for high-priority connections. |

## Authentication

Select Authentication and select a user group to require users to enter a user name and password before the firewall accepts the connection. Select the user group to control the users that can authenticate with this policy. To add and configure user groups, see [“Configuring user groups” on page 179](#). You must add user groups before you can select Authentication.

You can select Authentication for any service. Users can authenticate with the firewall using HTTP, Telnet, or FTP. For users to be able to authenticate you must add an HTTP, Telnet, or FTP policy that is configured for authentication. When users attempt to connect through the firewall using this policy they are prompted to enter a firewall username and password.

If you want users to authenticate to use other services (for example POP3 or IMAP) you can create a service group that includes the services for which you want to require authentication as well as HTTP, Telnet, and FTP. Then users could authenticate with the policy using HTTP, Telnet, or FTP before using the other service.

In most cases you should make sure that users can use DNS through the firewall without authentication. If DNS is not available users cannot connect to a web, FTP, or Telnet server using a domain name.

## Anti-Virus & Web filter

Enable antivirus protection and web filter content filtering for traffic controlled by this policy. You can select Anti-Virus & Web filter if Service is set to ANY, HTTP, SMTP, POP3, IMAP, or FTP or to a service group that includes the HTTP, SMTP, POP3, IMAP, or FTP services.

Select a content profile to configure how antivirus protection and content filtering is applied to the policy. See [“Content profiles” on page 169](#).

**Figure 6: Adding a Transparent mode policy**

The screenshot shows the 'New Policy' configuration window in a firewall management interface. At the top, there are tabs for different traffic directions: Int->Ext, Int->DMZ, DMZ->Int, DMZ->Ext, Ext->Int, and Ext->DMZ. The 'Int->Ext' tab is selected. The 'New Policy' section contains the following fields and options:

- Source:** Internal\_Net (dropdown)
- Destination:** External\_All (dropdown)
- Schedule:** Always (dropdown)
- Service:** HTTP (dropdown)
- Action:** ACCEPT (dropdown)
- Traffic Shaping:**
  - ☒ Traffic Shaping
  - Guaranteed Bandwidth: 100 (KBytes/s)
  - Maximum Bandwidth: 100 (KBytes/s)
  - Traffic Priority: High (dropdown)
- Authentication:**
  - ☒ Authentication
  - User\_Group\_1 (dropdown)
- Anti-Virus & Web filter:**
  - ☒ Anti-Virus & Web filter
  - Content Profile: Scan (dropdown)
- Log Traffic:**
  - ☒ Log Traffic

At the bottom of the window are 'OK' and 'Cancel' buttons.

## Log Traffic

Select Log Traffic to write messages to the traffic log whenever the policy processes a connection. For more information about logging, see [“Logging and reporting” on page 249](#).

## Comments

Optionally add a description or other information about the policy. The comment can be up to 63 characters long, including spaces.

## Configuring policy lists

The firewall matches policies by searching for a match starting at the top of the policy list and moving down until it finds the first match. You must arrange policies in the policy list from more specific to more general.

For example, the default policy is a very general policy because it matches all connection attempts. When you create exceptions to this policy, you must add them to the policy list above the default policy. No policy below the default policy will ever be matched.

This section describes:

- [Policy matching in detail](#)
- [Changing the order of policies in a policy list](#)
- [Enabling and disabling policies](#)

### Policy matching in detail

When the FortiGate unit receives a connection attempt at an interface, it must select a policy list to search through for a policy that matches the connection attempt. The FortiGate unit chooses the policy list based on the source and destination addresses of the connection attempt.

The FortiGate unit then starts at the top of the selected policy list and searches down the list for the first policy that matches the connection attempt source and destination addresses, service port, and time and date at which the connection attempt was received. The first policy that matches is applied to the connection attempt. If no policy matches, the connection is dropped.

The default policy accepts all connection attempts from the internal network to the Internet. From the internal network, users can browse the web, use POP3 to get email, use FTP to download files through the firewall, and so on. If the default policy is at the top of the Int->Ext policy list, the firewall allows all connections from the internal network to the Internet because all connections match the default policy. If more specific policies are added to the list below the default policy, they are never matched.

A policy that is an exception to the default policy, for example, a policy to block FTP connections, must be placed above the default policy in the Int->Ext policy list. In this example, all FTP connection attempts from the internal network would then match the FTP policy and be blocked. Connection attempts for all other kinds of services would not match with the FTP policy but they would match with the default policy. Therefore, the firewall would still accept all other connections from the internal network.



**Note:** Policies that require authentication must be added to the policy list above matching policies that do not; otherwise, the policy that does not require authentication is selected first.

### Changing the order of policies in a policy list

- 1 Go to **Firewall > Policy**.
- 2 Select the policy list that you want to rearrange.
- 3 Choose a policy to move and select Move To  to change its order in the policy list.

- 4 Type a number in the Move to field to specify where in the policy list to move the policy and select OK.

## Enabling and disabling policies

You can enable and disable policies in the policy list to control whether the policy is active or not. The FortiGate unit matches enabled policies but does not match disabled policies.

### Disabling a policy

Disable a policy to temporarily prevent the firewall from selecting the policy. Disabling a policy does not stop active communications sessions that have been allowed by the policy. To stop active communication sessions, see [“System status” on page 86](#).

- 1 Go to **Firewall > Policy**.
- 2 Select the policy list containing the policy to disable.
- 3 Clear the check box of the policy to disable.

### Enabling a policy

Enable a policy that has been disabled so that the firewall can match connections with the policy.

- 1 Go to **Firewall > Policy**.
- 2 Select the policy list containing the policy to enable.
- 3 Select the check box of the policy to enable.

## Addresses

All policies require source and destination addresses. To add addresses to a policy between two interfaces, you must first add addresses to the address list for each interface.

You can add, edit, and delete all firewall addresses as required. You can also organize related addresses into address groups to simplify policy creation.

A firewall address consists of an IP address and a netmask. This information can represent:

- The address of a subnet (for example, for a class C subnet, IP address: 192.168.20.0 and Netmask: 255.255.255.0).
- A single IP address (for example, IP Address: 192.168.20.1 and Netmask: 255.255.255.255)
- All possible IP addresses (represented by IP Address: 0.0.0.0 and Netmask: 0.0.0.0)



**Note:** IP address: 0.0.0.0 and Netmask: 255.255.255.255 is not a valid firewall address.

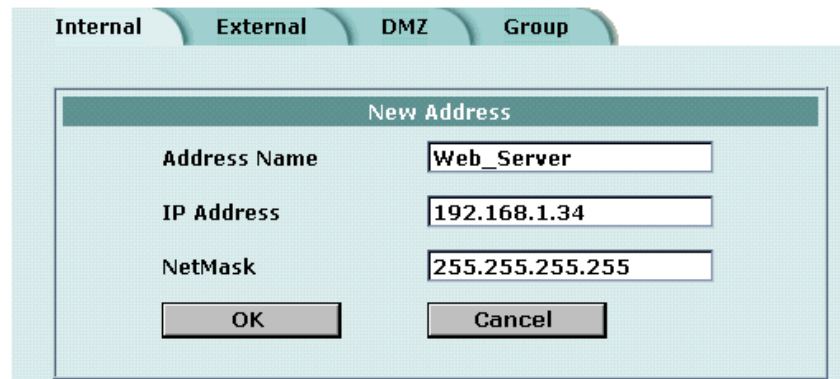
This section describes:

- [Adding addresses](#)
- [Editing addresses](#)
- [Deleting addresses](#)
- [Organizing addresses into address groups](#)

## Adding addresses

- 1 Go to **Firewall > Address**.
  - 2 Select the interface to which to add the address.
  - 3 Select New to add a new address.
  - 4 Enter an Address Name to identify the address.  
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Spaces and other special characters are not allowed.
  - 5 Enter the IP Address.  
The IP address can be:
    - The IP address of a single computer (for example, 192.45.46.45).
    - The IP address of a subnetwork (for example, 192.168.1.0 for a class C subnet).
    - 0.0.0.0 to represent all possible IP addresses
  - 6 Enter the NetMask.  
The netmask should correspond to the type of address that you are adding. For example:
    - The netmask for the IP address of a single computer should be 255.255.255.255.
    - The netmask for a class A subnet should be 255.0.0.0.
    - The netmask for a class B subnet should be 255.255.0.0.
    - The netmask for a class C subnet should be 255.255.255.0.
    - The netmask for all addresses should be 0.0.0.0
-  **Note:** To add an address to represent any address on a network set the IP Address to 0.0.0.0 and the Netmask to 0.0.0.0
- To add an address
- 7 Select OK to add the address.

Figure 7: Adding an internal address



The screenshot shows a 'New Address' dialog box with the following fields and values:

| Field        | Value           |
|--------------|-----------------|
| Address Name | Web_Server      |
| IP Address   | 192.168.1.34    |
| NetMask      | 255.255.255.255 |

Buttons: OK, Cancel

## Editing addresses

Edit an address to change its IP address and netmask. You cannot edit the address name. To change the address name, you must delete the address entry and then add the address again with a new name.

- 1 Go to **Firewall > Address**.
- 2 Select the interface list containing the address that you want to edit.
- 3 Choose an address to edit and select Edit Address .
- 4 Make the required changes and select OK to save your changes.

## Deleting addresses

Deleting an address removes it from an address list. To delete an address that has been added to a policy, you must first remove the address from the policy.

- 1 Go to **Firewall > Address**.
- 2 Select the interface list containing the address that you want to delete. You can delete any listed address that has a Delete Address icon .
- 3 Choose an address to delete and select Delete .
- 4 Select OK to delete the address.

## Organizing addresses into address groups

You can organize related addresses into address groups to make it easier to add policies. For example, if you add three addresses and then add them to an address group, you only have to add one policy using the address group rather than a separate policy for each address.

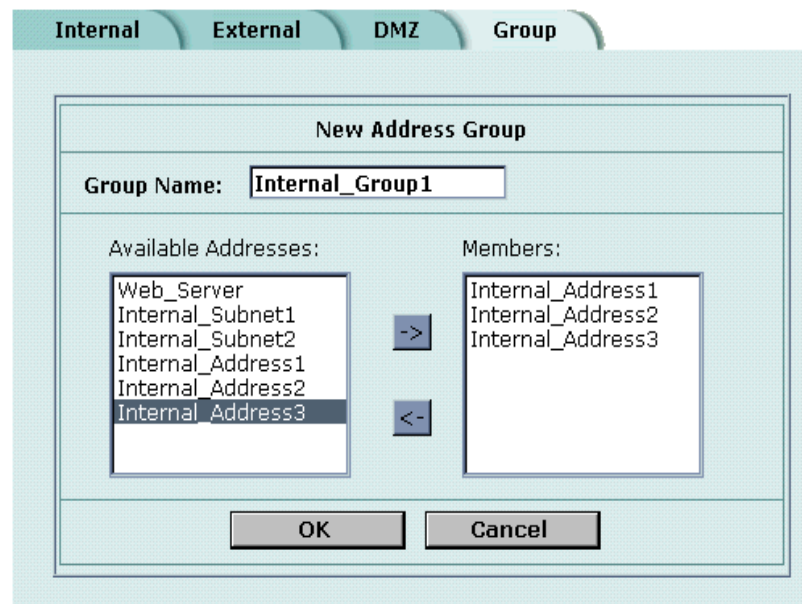
You can add address groups to any interface. The address group can only contain addresses from that interface. Address groups are available in interface source or destination address lists.

Address groups cannot have the same names as individual addresses. If an address group is included in a policy, it cannot be deleted unless it is first removed from the policy.

- 1 Go to **Firewall > Address > Group**.

- 2 Select the interface to which to add the address group.
- 3 Enter a Group Name to identify the address group.  
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.
- 4 To add addresses to the address group, select an address from the Available Addresses list and select the right arrow to add it to the Members list.
- 5 To remove addresses from the address group, select an address from the Members list and select the left arrow to remove it from the group.
- 6 Select OK to add the address group.

**Figure 8: Adding an internal address group**



## Services

Use services to control the types of communication accepted or denied by the firewall. You can add any of the predefined services to a policy. You can also create your own custom services and add services to service groups.

This section describes:

- [Predefined services](#)
- [Providing access to custom services](#)
- [Grouping services](#)

### Predefined services

The FortiGate predefined firewall services are listed in [Table 5](#). You can add these services to any policy.

**Table 5: FortiGate predefined services**

| Service name             | Description                                                                                                                                                                                                       | Protocol | Port       |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------------|
| ANY                      | Match connections on any port. A connection that uses any of the predefined services is allowed through the firewall.                                                                                             | all      | all        |
| GRE                      | Generic Routing Encapsulation. A protocol that allows an arbitrary network protocol to be transmitted over any other arbitrary network protocol, by encapsulating the packets of the protocol within GRE packets. |          | 47         |
| AH                       | Authentication Header. AH provides source host authentication and data integrity, but not secrecy. This protocol is used for authentication by IPSec remote gateways set to aggressive mode.                      |          | 51         |
| ESP                      | Encapsulating Security Payload. This service is used by manual key and AutoIKE VPN tunnels for communicating encrypted data. AutoIKE key VPN tunnels use ESP after establishing the tunnel using IKE.             |          | 50         |
| AOL                      | AOL instant messenger protocol.                                                                                                                                                                                   | tcp      | 5190-5194  |
| BGP                      | Border Gateway Protocol routing protocol. BGP is an interior/exterior routing protocol.                                                                                                                           | tcp      | 179        |
| DHCP-Relay               | Dynamic Host Configuration Protocol (DHCP) allocates network addresses and delivers configuration parameters from DHCP servers to hosts.                                                                          | udp      | 67         |
| DNS                      | Domain name service for translating domain names into IP addresses.                                                                                                                                               | tcp      | 53         |
|                          |                                                                                                                                                                                                                   | udp      | 53         |
| FINGER                   | A network service that provides information about users.                                                                                                                                                          | tcp      | 79         |
| FTP                      | FTP service for transferring files.                                                                                                                                                                               | tcp      | 21         |
| GOPHER                   | Gopher communication service. Gopher organizes and displays Internet server contents as a hierarchically structured list of files.                                                                                | tcp      | 70         |
| H323                     | H.323 multimedia protocol. H.323 is a standard approved by the International Telecommunication Union (ITU) that defines how audiovisual conferencing data is transmitted across networks.                         | tcp      | 1720, 1503 |
| HTTP                     | HTTP is the protocol used by the word wide web for transferring data for web pages.                                                                                                                               | tcp      | 80         |
| HTTPS                    | HTTP with secure socket layer (SSL) service for secure communication with web servers.                                                                                                                            | tcp      | 443        |
| IKE                      | IKE is the protocol to obtain authenticated keying material for use with ISAKMP for IPSEC.                                                                                                                        | udp      | 500        |
| IMAP                     | Internet Message Access Protocol is a protocol used for retrieving email messages.                                                                                                                                | tcp      | 143        |
| Internet-Locator-Service | Internet Locator Service includes LDAP, User Locator Service, and LDAP over TLS/SSL.                                                                                                                              | tcp      | 389        |

**Table 5: FortiGate predefined services (Continued)**

| Service name | Description                                                                                                                                                      | Protocol | Port                       |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|----------------------------|
| IRC          | Internet Relay Chat allows people connected to the Internet to join live discussions.                                                                            | tcp      | 6660-6669                  |
| L2TP         | L2TP is a PPP-based tunnel protocol for remote access.                                                                                                           | tcp      | 1701                       |
| LDAP         | Lightweight Directory Access Protocol is a set of protocols used to access information directories.                                                              | tcp      | 389                        |
| NetMeeting   | NetMeeting allows users to teleconference using the Internet as the transmission medium.                                                                         | tcp      | 1720                       |
| NFS          | Network File System allows network users to access shared files stored on computers of different types.                                                          | tcp      | 111, 2049                  |
| NNTP         | Network News Transport Protocol is a protocol used to post, distribute, and retrieve USENET messages.                                                            | tcp      | 119                        |
| NTP          | Network time protocol for synchronizing a computer's time with a time server.                                                                                    | tcp      | 123                        |
| OSPF         | Open Shortest Path First (OSPF) routing protocol. OSPF is a common link state routing protocol.                                                                  |          | 89                         |
| PC-Anywhere  | PC-Anywhere is a remote control and file transfer protocol.                                                                                                      | udp      | 5632                       |
| PING         | Packet Internet Groper is a utility to determine whether a specific host is accessible by its IP address.                                                        | icmp     | 8                          |
| POP3         | Post office protocol email protocol for downloading email from a POP3 server.                                                                                    | tcp      | 110                        |
| PPTP         | Point-to-Point Tunneling Protocol is a protocol that allows corporations to extend their own corporate network through private tunnels over the public Internet. | tcp      | 1723                       |
| QUAKE        | For connections used by the popular Quake multi-player computer game.                                                                                            | udp      | 26000, 27000, 27910, 27960 |
| RAUDIO       | For streaming real audio multimedia traffic.                                                                                                                     | udp      | 7070                       |
| RLOGIN       | Rlogin service for remotely logging into a server.                                                                                                               | tcp      | 513                        |
| RIP          | Routing Information Protocol is a common distance vector routing protocol.                                                                                       | udp      | 520                        |
| SMTP         | For sending mail between email servers on the Internet.                                                                                                          | tcp      | 25                         |
| SNMP         | Simple Network Management Protocol is a set of protocols for managing complex networks                                                                           | tcp      | 161-162                    |
|              |                                                                                                                                                                  | udp      | 161-162                    |
| SSH          | SSH service for secure connections to computers for remote management.                                                                                           | tcp      | 22                         |
|              |                                                                                                                                                                  | udp      | 22                         |
| SYSLOG       | Syslog service for remote logging.                                                                                                                               | udp      | 514                        |
| TALK         | A protocol supporting conversations between two or more users.                                                                                                   | udp      | 517-518                    |

**Table 5: FortiGate predefined services (Continued)**

| Service name | Description                                                                                                   | Protocol | Port      |
|--------------|---------------------------------------------------------------------------------------------------------------|----------|-----------|
| TCP          | All TCP ports.                                                                                                | tcp      | 0-65535   |
| TELNET       | Telnet service for connecting to a remote computer to run commands.                                           | tcp      | 23        |
| TFTP         | Trivial file transfer protocol, a simple file transfer protocol similar to FTP but with no security features. | udp      | 69        |
| UDP          | All UDP ports.                                                                                                | udp      | 0-65535   |
| UUCP         | Unix to Unix copy utility, a simple file copying protocol.                                                    | udp      | 540       |
| VDOLIVE      | For VDO Live streaming multimedia traffic.                                                                    | tcp      | 7000-7010 |
| WAIS         | Wide Area Information Server. An Internet search protocol.                                                    | tcp      | 210       |
| WINFRAME     | For WinFrame communications between computers running Windows NT.                                             | tcp      | 1494      |
| X-WINDOWS    | For remote communications between an X-Window server and X-Window clients.                                    | tcp      | 6000-6063 |

## Providing access to custom services

Add a custom service if you need to create a policy for a service that is not in the predefined service list.

- 1 Go to **Firewall > Service > Custom**.
- 2 Select New.
- 3 Enter a Name for the service. This name appears in the service list used when you add a policy.  
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.
- 4 Select the Protocol (either TCP or UDP) used by the service.
- 5 Specify a Source and Destination Port number range for the service by entering the low and high port numbers. If the service uses one port number, enter this number in both the low and high fields.
- 6 If the service has more than one port range, select Add to specify additional protocols and port ranges.  
If you mistakenly add too many port range rows, select Delete  to remove each extra row.
- 7 Select OK to add the custom service.  
You can now add this custom service to a policy.

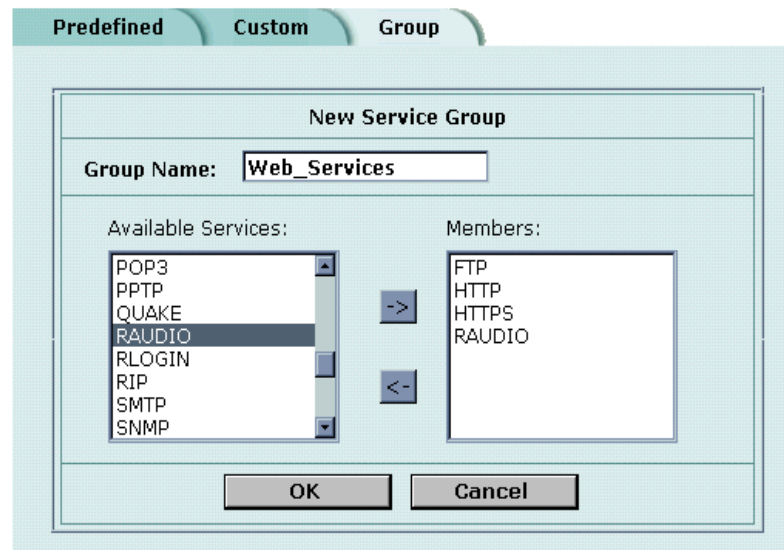
## Grouping services

To make it easier to add policies, you can create groups of services and then add one policy to provide or block access for all the services in the group. A service group can contain predefined services and custom services in any combination. You cannot add service groups to another service group.

- 1 Go to **Firewall > Service > Group**.

- 2 Select New.
- 3 Enter a Group Name to identify the group.  
This name appears in the service list when you add a policy and cannot be the same as a predefined service name.  
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.
- 4 To add services to the service group, select a service from the Available Services list and select the right arrow to copy it to the Members list.
- 5 To remove services from the service group, select a service from the Members list and select the left arrow to remove it from the group.
- 6 Select OK to add the service group.

**Figure 9: Adding a service group**



## Schedules

Use scheduling to control when policies are active or inactive. You can create one-time schedules and recurring schedules. You can use one-time schedules to create policies that are effective once for the period of time specified in the schedule. Recurring schedules repeat weekly. You can use recurring schedules to create policies that are effective only at specified times of the day or on specified days of the week.

This section describes:

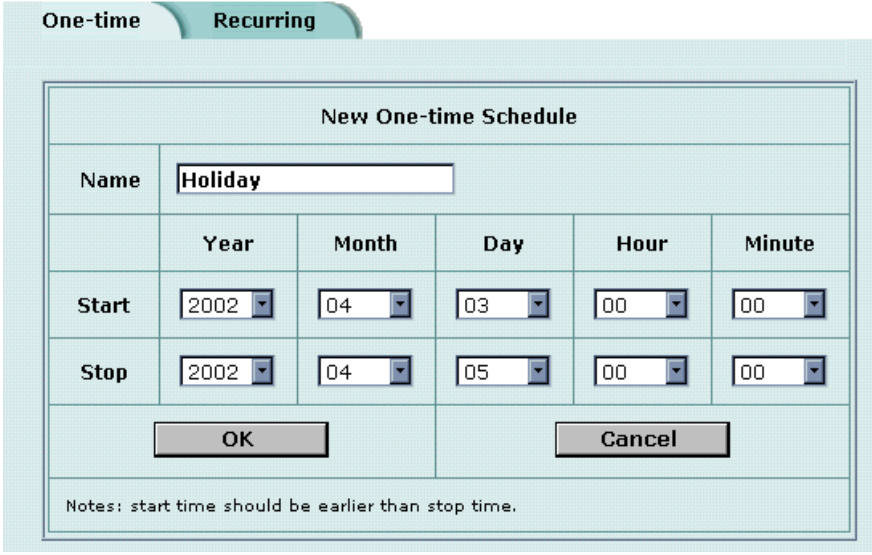
- [Creating one-time schedules](#)
- [Creating recurring schedules](#)
- [Adding a schedule to a policy](#)

## Creating one-time schedules

You can create a one-time schedule that activates or deactivates a policy for a specified period of time. For example, your firewall might be configured with the default policy that allows access to all services on the Internet at all times. You can add a one-time schedule to block access to the Internet during a holiday period.

- 1 Go to **Firewall > Schedule > One-time**.
- 2 Select New.
- 3 Enter a Name for the schedule.  
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.
- 4 Set the Start date and time for the schedule.  
Set Start and Stop times to 00 for the schedule to be active for the entire day.
- 5 Set the Stop date and time for the schedule.  
One-time schedules use the 24-hour clock.
- 6 Select OK to add the one-time schedule.

**Figure 10: Adding a one-time schedule**



| New One-time Schedule                               |         |       |        |      |        |
|-----------------------------------------------------|---------|-------|--------|------|--------|
| Name                                                | Holiday |       |        |      |        |
|                                                     | Year    | Month | Day    | Hour | Minute |
| Start                                               | 2002    | 04    | 03     | 00   | 00     |
| Stop                                                | 2002    | 04    | 05     | 00   | 00     |
| OK                                                  |         |       | Cancel |      |        |
| Notes: start time should be earlier than stop time. |         |       |        |      |        |

## Creating recurring schedules

You can create a recurring schedule that activates or deactivates policies at specified times of the day or on specified days of the week. For example, you might want to prevent Internet use outside of working hours by creating a recurring schedule.

If you create a recurring schedule with a stop time that occurs before the start time, the schedule will start at the start time and finish at the stop time on the next day. You can use this technique to create recurring schedules that run from one day to the next. You can also create a recurring schedule that runs for 24 hours by setting the start and stop times to the same time.

- 1 Go to **Firewall > Schedule > Recurring**.
- 2 Select New to create a new schedule.

- 3 Enter a Name for the schedule.  
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.
- 4 Select the days of the week on which the schedule should be active.
- 5 Set the Start and Stop hours in between which the schedule should be active.  
Recurring schedules use the 24-hour clock.
- 6 Select OK to save the recurring schedule.

Figure 11: Adding a recurring schedule

| New Recurring Schedule                                                                                                                                                              |                          |                                     |                                     |                                     |                                     |                                     |                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|
| Name                                                                                                                                                                                | Working_Week             |                                     |                                     |                                     |                                     |                                     |                          |
| Day                                                                                                                                                                                 | Sun                      | Mon                                 | Tue                                 | Wed                                 | Thu                                 | Fri                                 | Sat                      |
| Select                                                                                                                                                                              | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Start                                                                                                                                                                               | Hour                     |                                     | 08                                  | Minute                              |                                     | 00                                  |                          |
| Stop                                                                                                                                                                                | Hour                     |                                     | 17                                  | Minute                              |                                     | 00                                  |                          |
| OK                                                                                                                                                                                  |                          |                                     |                                     | Cancel                              |                                     |                                     |                          |
| Notes: If the stop time is set earlier than the start time, the stop time will be during next day. If the start time is equal to the stop time, the schedule will run for 24 hours. |                          |                                     |                                     |                                     |                                     |                                     |                          |

## Adding a schedule to a policy

After you have created schedules, you can add them to policies to schedule when the policies are active. You can add the new schedules to policies when you create the policy, or you can edit existing policies and add a new schedule to them.

- 1 Go to **Firewall > Policy**.
- 2 Select the tab corresponding to the type of policy to add.
- 3 Select New to add a policy or select Edit  to edit a policy to change its schedule.
- 4 Configure the policy as required.
- 5 Add a schedule by selecting it from the Schedule list.
- 6 Select OK to save the policy.
- 7 Arrange the policy in the policy list to have the effect that you expect.

For example, to use a one-time schedule to deny access to a policy, add a policy that matches the policy to be denied in every way. Choose the one-time schedule that you added and set Action to DENY. Then place the policy containing the one-time schedule in the policy list above the policy to be denied.

## Virtual IPs

Use virtual IPs to access IP addresses on a destination network that are hidden from the source network by NAT security policies. To allow connections between these networks, you must create a mapping between an address on the source network and the real address on the destination network. This mapping is called a virtual IP.

For example, if the computer hosting your web server is located on your DMZ network, it could have a private IP address such as 10.10.10.3. To get packets from the Internet to the web server, you must have an external address for the web server on the Internet. You must then add a virtual IP to the firewall that maps the external IP address of the web server to the actual address of the web server on the DMZ network. To allow connections from the Internet to the web server, you must then add an Ext->DMZ firewall policy and set Destination to the virtual IP.

You can create two types of virtual IPs:

**Static NAT** Used in to translate an address on a source network to a hidden address on a destination network. Static NAT translates the source address of return packets to the address on the source network.

**Port Forwarding** Used to translate an address and a port number on a source network to a hidden address and, optionally, a different port number on a destination network. Using port forwarding you can also route packets with a specific port number and a destination address that matches the IP address of the interface that receives the packets. This technique is called port forwarding or port address translation (PAT). You can also use port forwarding to change the destination port of the forwarded packets.

This section describes:

- [Adding static NAT virtual IPs](#)
- [Adding port forwarding virtual IPs](#)
- [Adding policies with virtual IPs](#)

### Adding static NAT virtual IPs

- 1 Go to **Firewall > Virtual IP**.
- 2 Select New to add a virtual IP.
- 3 Enter a Name for the virtual IP.  
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.
- 4 Select the virtual IP External Interface:  
The External Interface is the interface connected to the source network that receives the packets to be forwarded to the destination network.
- 5 Make sure Type is set to Static NAT.

- 6 In the External IP Address field, enter the external IP address to be mapped to an address on the destination network.  
 For example, if the virtual IP provides access from the Internet to a web server on a destination network, the external IP address must be a static IP address obtained from your ISP for your web server. This address must be a unique address that is not used by another host and cannot be the same as the IP address of the External Interface selected in step 4. However, this address must be routed to this interface.  
 If the IP address of the External interface selected in step 4 is set using PPPoE or DHCP, you can enter 0.0.0.0 for the External IP Address. The FortiGate unit substitutes the IP address set for this external interface using PPPoE or DHCP.

**Figure 12: Adding a static NAT virtual IP**

- 7 In the Map to IP field, enter the real IP address on the destination network, for example, the IP address of a web server on an internal network.



**Note:** The firewall translates the source address of outbound packets from the host with the Map to IP address to the virtual IP External IP Address, instead of the firewall external address.

- 8 Select OK to save the virtual IP.  
 You can now add the virtual IP to firewall policies.

## Adding port forwarding virtual IPs

- 1 Go to **Firewall > Virtual IP**.
- 2 Select New to add a virtual IP.
- 3 Enter a Name for the virtual IP.  
 The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.

- 4** Select the virtual IP External Interface. The External Interface is the interface connected to the source network that receives the packets to be forwarded to the destination network.
- 5** Change Type to Port Forwarding.
- 6** In the External IP Address field, enter the external IP address to be mapped to an address on the destination zone.  
You can set the External IP Address to the IP address of external interface selected in step 4 or to any other address.  
If the IP address of the External interface selected in step 4 is set using PPPoE or DHCP, you can enter 0.0.0.0 for the External IP Address. The FortiGate unit substitutes the IP address set for this external interface using PPPoE or DHCP.  
For example, if the virtual IP provides access from the Internet to a server on your internal network, the External IP Address must be a static IP address obtained from your ISP for this server. This address must be a unique address that is not used by another host. However, this address must be routed to the External Interface selected in step 4.
- 7** Enter the External Service Port number for which to configure port forwarding.  
The external service port number must match the destination port of the packets to be forwarded. For example, if the virtual IP provides access from the Internet to a Web server, the external service port number would be 80 (the HTTP port).
- 8** In Map to IP, enter the real IP address on the destination network.  
For example, the real IP address could be the IP address of a web server on an internal network.  
If you enter an IP address on the same subnet as the internal interface, the virtual IP can be added to Ext->Int or DMZ->Int policies.  
If you enter an IP address on the same subnet as the DMZ interface, the virtual IP can be added to Ext->DMZ policies.
- 9** Set Map to Port to the port number to be added to packets when they are forwarded.  
If you do not want to translate the port, enter the same number as the External Service Port.  
If you want to translate the port, enter the port number to which to translate the destination port of the packets when they are forwarded by the firewall.
- 10** Select the protocol to be used by the forwarded packets.
- 11** Select OK to save the port forwarding virtual IP.

Figure 13: Adding a port forwarding virtual IP

**Virtual IP**

**Add New Virtual IP Mapping**

Name:

External Interface:

Type: ☐ Static NAT ☒ Port Forwarding

External IP Address:

External Service Port:

Map to IP:

Map to Port:

Protocol: ☒ TCP ☐ UDP

## Adding policies with virtual IPs

Use the following procedure to add a policy that uses a virtual IP to forward packets.

- 1 Go to **Firewall > Policy**.
- 2 Select the type of policy to add.
  - The source interface must match the interface selected in the External Interface list.
  - The destination interface must match the interface connected to the network with the Map to IP address.
- 3 Use the following information to configure the policy.

|                    |                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Source</b>      | Select the source address from which users can access the server.                                                  |
| <b>Destination</b> | Select the virtual IP.                                                                                             |
| <b>Schedule</b>    | Select a schedule as required.                                                                                     |
| <b>Service</b>     | Select the service that matches the Map to Service that you selected for the port-forwarding virtual IP.           |
| <b>Action</b>      | Set action to ACCEPT to accept connections to the internal server. You can also select DENY to deny access.        |
| <b>NAT</b>         | Select NAT if the firewall is protecting the private addresses on the destination network from the source network. |

|                                    |                                                                                                                                                                |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authentication</b>              | Optionally select Authentication and select a user group to require users to authenticate with the firewall before accessing the server using port forwarding. |
| <b>Log Traffic</b>                 | Select these options to log port-forwarded traffic and apply antivirus and web filter protection to this traffic.                                              |
| <b>Anti-Virus &amp; Web filter</b> |                                                                                                                                                                |

- 4 Select OK to save the policy.

## IP pools

An IP pool (also called a dynamic IP pool) is a range of IP addresses added to a firewall interface. If you add IP pools to an interface, you can select Dynamic IP Pool when you configure a policy with the destination set to this interface. You can add an IP pool if you want to add NAT mode policies that translate source addresses to addresses randomly selected from the IP pool rather than being limited to the IP address of the destination interface.

For example, if you add an IP pool to the internal interface, you can select Dynamic IP pool for Ext->Int and DMZ->Int policies.

The addresses in the IP pool must be on the same subnet as the IP address of the interface. For example, if the IP address of a FortiGate interface is 192.168.1.99, a valid IP pool could start IP at 192.168.1.10 and end at 192.168.1.20. This IP pool would give the firewall 11 addresses to select from when translating the source address.

The addresses in the IP pool range cannot conflict with other addresses on the same network as the interface for which you are adding the IP pool.

You can add multiple IP pools to any interface, but only the first IP pool is used by the Firewall.

This section describes:

- [Adding an IP pool](#)
- [IP Pools for firewall policies that use fixed ports](#)
- [IP pools and dynamic NAT](#)

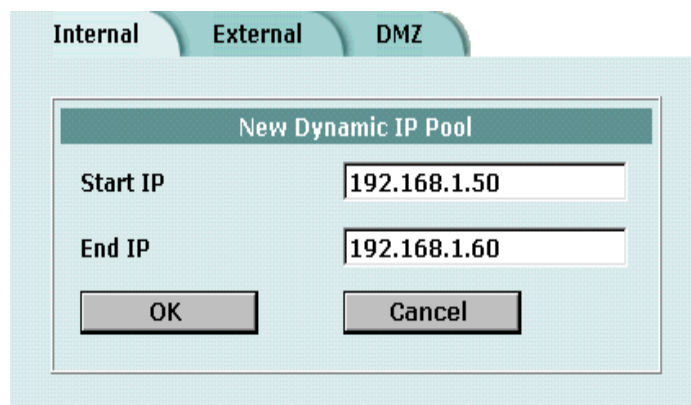
### Adding an IP pool

To add an IP pool:

- 1 Go to **Firewall > IP Pool**.
- 2 Select the interface to which to add the IP pool.
- 3 Select New to add a new IP pool to the selected interface.
- 4 Enter the Start IP and End IP addresses for the range of addresses in the IP pool.  
The Start IP and End IP must define the start and end of an address range. The Start IP must be lower than the End IP. The Start IP and End IP must be on the same subnet as the IP address of the interface for which you are adding the IP pool.  
If you have configured the external interface to use PPPoE or DHCP, you can only set the Start IP and End IP to the current IP address of the external interface.

- 5 Select OK to save the IP pool.

Figure 14: Adding an IP Pool



The screenshot shows a 'New Dynamic IP Pool' dialog box. At the top, there are three tabs: 'Internal', 'External', and 'DMZ'. The 'Internal' tab is selected. Below the tabs, the dialog has two input fields: 'Start IP' with the value '192.168.1.50' and 'End IP' with the value '192.168.1.60'. At the bottom, there are two buttons: 'OK' and 'Cancel'.

## IP Pools for firewall policies that use fixed ports

Some network configurations will not operate correctly if a NAT policy translates the source port of packets used by the connection. NAT translates source ports to keep track of connections for a particular service. You can select fixed port for NAT policies to prevent source port translation. However, selecting fixed port means that only one connection can be supported through the firewall for this service. To be able to support multiple connections, you can add an IP pool to the destination interface, and then select Dynamic P pool in the policy. The firewall randomly selects an IP address from the IP pool and assigns it to each connection. In this case the number of connections that the firewall can support is limited by the number of IP addresses in the IP pool.

## IP pools and dynamic NAT

You can use IP pools for dynamic NAT. For example, your organization may have purchased a range of Internet addresses, but you may have only one Internet connection: the external interface of your FortiGate unit.

You can assign one of your organization's Internet IP addresses to the external interface of your FortiGate unit. If your FortiGate unit is operating in NAT/Route mode, all connections from your network to the Internet appear to come from this IP address.

If you want connections to originate from all of your Internet IP addresses, you can add this address range to an IP pool for the external interface. Then you can select Dynamic IP Pool for all policies with the external interface as the destination. For each connection the firewall dynamically selects an IP address from the IP pool to be the source address for the connection. As a result connections to the Internet will appear to be originating from all of the IP addresses in the IP pool.

## IP/MAC binding

IP/MAC binding protects the FortiGate unit and your network from IP spoofing attacks. IP spoofing attempts to use the IP address of a trusted computer to connect to or through the FortiGate unit from a different computer. The IP address of a computer can easily be changed to a trusted address, but MAC addresses are added to Ethernet cards at the factory and cannot easily be changed.

You can enter the static IP addresses and corresponding MAC addresses of trusted computers in the Static IP/MAC table.

If you have trusted computers with dynamic IP addresses that are set by the FortiGate DHCP server, the FortiGate unit adds these IP addresses and their corresponding MAC addresses to the Dynamic IP/MAC table. See [“Providing DHCP services to your internal network” on page 119](#). The dynamic IP/MAC binding table is not available in Transparent mode.

IP/MAC binding can be enabled for packets connecting to the firewall or passing through the firewall.



**Note:** If you enable IP/MAC binding and change the IP address of a computer with an IP or MAC address in the IP/MAC list, you must also change the entry in the IP/MAC list or the computer will not have access to or through the FortiGate unit. You must also add the IP/MAC address pair of any new computer that you add to your network or this computer will not have access to or through the FortiGate unit.

This section describes:

- [Configuring IP/MAC binding for packets going through the firewall](#)
- [Configuring IP/MAC binding for packets going to the firewall](#)
- [Adding IP/MAC addresses](#)
- [Viewing the dynamic IP/MAC list](#)
- [Enabling IP/MAC binding](#)

### Configuring IP/MAC binding for packets going through the firewall

Use the following procedure to use IP/MAC binding to filter packets that would normally be allowed through the firewall by a firewall policy.

- 1 Go to **Firewall > IP/MAC Binding > Setting**.
- 2 Select Enable IP/MAC binding going through the firewall.
- 3 Go to **Firewall > IP/MAC Binding > Static IP/MAC**.
- 4 Select New to add IP/MAC binding pairs to the IP/MAC binding list.

All packets that would normally be allowed through the firewall by a firewall policy are first compared with the entries in the IP/MAC binding list. If a match is found, then the firewall attempts to match the packet with a policy.

For example, if the IP/MAC pair IP 1.1.1.1 and 12:34:56:78:90:ab:cd is added to the IP/MAC binding list:

- A packet with IP address 1.1.1.1 and MAC address 12:34:56:78:90:ab:cd is allowed to go on to be matched with a firewall policy.
- A packet with IP 1.1.1.1 but with a different MAC address is dropped immediately to prevent IP spoofing.
- A packet with a different IP address but with a MAC address of 12:34:56:78:90:ab:cd is dropped immediately to prevent IP spoofing.
- A packet with both the IP address and MAC address not defined in the IP/MAC binding table:
  - is allowed to go on to be matched with a firewall policy if IP/MAC binding is set to Allow traffic,
  - is blocked if IP/MAC binding is set to Block traffic.

## Configuring IP/MAC binding for packets going to the firewall

Use the following procedure to use IP/MAC binding to filter packets that would normally connect with the firewall (for example, when an administrator is connecting to the FortiGate unit for management).

- 1 Go to **Firewall > IP/MAC Binding > Setting**.
- 2 Select Enable IP/MAC binding going to the firewall.
- 3 Go to **Firewall > IP/MAC Binding > Static IP/MAC**.
- 4 Select New to add IP/MAC binding pairs to the IP/MAC binding list.

All packets that would normally connect to the firewall are first compared with the entries in the IP/MAC binding table.

For example, if the IP/MAC pair IP 1.1.1.1 and 12:34:56:78:90:ab:cd is added to the IP/MAC binding list:

- A packet with IP address 1.1.1.1 and MAC address 12:34:56:78:90:ab:cd is allowed to connect to the firewall.
- A packet with IP 1.1.1.1 but with a different MAC address is dropped immediately to prevent IP spoofing.
- A packet with a different IP address but with a MAC address of 12:34:56:78:90:ab:cd is dropped immediately to prevent IP spoofing.
- A packet with both the IP address and MAC address not defined in the IP/MAC binding table:
  - is allowed to connect to the firewall if IP/MAC binding is set to Allow traffic,
  - is blocked if IP/MAC binding is set to Block traffic.

## Adding IP/MAC addresses

- 1 Go to **Firewall > IP/MAC Binding > Static IP/MAC**.
- 2 Select New to add an IP address/MAC address pair.

- 3 Enter the IP address and the MAC address.  
You can bind multiple IP addresses to the same MAC address. You cannot bind multiple MAC addresses to the same IP address.  
However, you can set the IP address to 0.0.0.0 for multiple MAC addresses. This means that all packets with these MAC addresses are matched with the IP/MAC binding list.  
Similarly, you can set the MAC address to 00:00:00:00:00:00 for multiple IP addresses. This means that all packets with these IP addresses are matched with the IP/MAC binding list.
- 4 Enter a Name for the new IP/MAC address pair.  
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.
- 5 Select Enable to enable IP/MAC binding for the IP/MAC pair.
- 6 Select OK to save the IP/MAC binding pair.

## Viewing the dynamic IP/MAC list

- 1 Go to **Firewall > IP/MAC Binding > Dynamic IP/MAC**.

## Enabling IP/MAC binding



**Caution:** Make sure that you have added the IP/MAC Address pair of your management computer before enabling IP/MAC binding.

- 1 Go to **Firewall > IP/MAC Binding > Setting**.
- 2 Select Enable IP/MAC binding going through the firewall to turn on IP/MAC binding for packets that could be matched by policies.
- 3 Select Enable IP/MAC binding going to the firewall to turn on IP/MAC binding for packets connecting to the firewall.
- 4 Configure how IP/MAC binding handles packets with IP and MAC addresses that are not defined in the IP/MAC list.  
Select Allow traffic to allow all packets with IP and MAC address pairs that are not added to the IP/MAC binding list.  
Select Block traffic to block packets with IP and MAC address pairs that are not added to the IP/MAC binding list.
- 5 Select Apply to save your changes.

**Figure 15: IP/MAC settings**

Setting Static IP/MAC Dynamic IP/MAC

☒ Enable IP/MAC binding going through the firewall.

☒ Enable IP/MAC binding going to the firewall.

For hosts not defined in table:

☐ Allow traffic.

☒ Block traffic.

Apply

## Content profiles

Use content profiles to apply different protection settings for content traffic controlled by firewall policies. You can use content profiles to:

- Configure antivirus protection for HTTP, FTP, POP3, SMTP, and IMAP policies
- Configure web filtering for HTTP policies
- Configure email filtering for IMAP and POP3 policies
- Configure oversized file and email blocking for HTTP, FTP, POP3, SMTP, and IMAP policies
- Passing fragmented email for POP3, SMTP, and IMAP policies

Using content profiles you can build up protection configurations that can be easily applied to different types of Firewall policies. This allows you to customize different types and different levels of protection for different firewall policies.

For example, while traffic between internal and external addresses might need strict protection, traffic between trusted internal addresses might need moderate protection. You can configure policies for different traffic services to use the same or different content profiles.

Content profiles can be added to NAT/Route mode and Transparent mode policies.

- [Default content profiles](#)
- [Adding a content profile](#)
- [Adding a content profile to a policy](#)

## Default content profiles

The FortiGate unit has the following four default content profiles under **Firewall > Content Profile**. You can use these existing content profiles or create your own:

|                   |                                                                                                                                                                                                                                                                                        |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Strict</b>     | To apply maximum content protection to HTTP, FTP, IMAP, POP3, and SMTP content traffic. You would not use the strict content profile under normal circumstances, but it is available if you are having extreme problems with viruses and require maximum content screening protection. |
| <b>Scan</b>       | Apply antivirus scanning to HTTP, FTP, IMAP, POP3, and SMTP content traffic.                                                                                                                                                                                                           |
| <b>Web</b>        | Apply antivirus scanning and Web content blocking to HTTP content traffic. You can add this content profile to firewall policies that control HTTP traffic.                                                                                                                            |
| <b>Unfiltered</b> | Use the unfiltered content profile if you do not want to apply any content protection to content traffic. You can add this content profile to firewall policies for connections between highly trusted or highly secure networks where content does not need to be protected.          |

## Adding a content profile

If the default content profiles do not provide the protection that you require, you can create new content profiles customized to your requirements.

- 1 Go to **Firewall > Content Profile**.
- 2 Select New.
- 3 Type a Profile Name.
- 4 Enable antivirus protection options.

|                        |                                                                                                                                                                                                                                                        |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Anti Virus Scan</b> | Scan web, FTP, and email traffic for viruses and worms. See <a href="#">“Antivirus scanning” on page 232</a> .                                                                                                                                         |
| <b>File Block</b>      | Delete files with blocked file patterns even if they do not contain viruses. You should only enable file blocking when a virus has been found that is so new that virus scanning does not detect it. See <a href="#">“File blocking” on page 233</a> . |



**Note:** If both virus Scan and File Block are enabled, the FortiGate unit blocks files that match enabled file patterns before they are scanned for viruses.

- 5 Enable Web filtering options.

|                          |                                                                                                                                                                                                                                                                        |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Web URL Block</b>     | Block unwanted web pages and web sites. This option adds Fortinet URL blocking (see <a href="#">“URL blocking” on page 237</a> ) and Cerberian URL filtering (see <a href="#">“Using the Cerberian web filter” on page 240</a> ) to HTTP traffic accepted by a policy. |
| <b>Web Content Block</b> | Block web pages that contain unwanted words or phrases. See <a href="#">“Content blocking” on page 236</a> .                                                                                                                                                           |
| <b>Web Script Filter</b> | Remove scripts from web pages. See <a href="#">“Script filtering” on page 242</a> .                                                                                                                                                                                    |
| <b>Web Exempt List</b>   | Exempt URLs from web filtering and virus scanning. See <a href="#">“Exempt URL list” on page 243</a> .                                                                                                                                                                 |

- 6 Enable Email filter protection options.

|                          |                                                                                                            |
|--------------------------|------------------------------------------------------------------------------------------------------------|
| <b>Email Block List</b>  | Add a subject tag to email from unwanted addresses. See <a href="#">“Email block list” on page 247</a> .   |
| <b>Email Exempt List</b> | Exempt sender address patterns from email filtering. See <a href="#">“Email exempt list” on page 247</a> . |

- Email Content Block** Add a subject tag to email that contains unwanted words or phrases. See ["Email banned word list" on page 246](#).
- 7 Enable fragmented email and oversized file and email options.
- Oversized File/Email Block** Block or pass files and email that exceed thresholds configured as a percent of system memory. See ["Blocking oversized files and emails" on page 234](#).
- Pass Fragmented Email** Allow email messages that have been fragmented to bypass antivirus scanning. See ["Exempting fragmented email from blocking" on page 234](#).
- 8 Select OK.

Figure 16: Example content profile

Content Profile

**Edit Content Profile**

Profile Name:

| Options                | HTTP                                                                 | FTP                                                                  | IMAP                                                                 | POP3                                                                 | SMTP                                                                 |
|------------------------|----------------------------------------------------------------------|----------------------------------------------------------------------|----------------------------------------------------------------------|----------------------------------------------------------------------|----------------------------------------------------------------------|
| Anti Virus Scan        | <input checked="" type="checkbox"/>                                  | <input checked="" type="checkbox"/>                                  | <input checked="" type="checkbox"/>                                  | <input checked="" type="checkbox"/>                                  | <input checked="" type="checkbox"/>                                  |
| File Block             | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             |
| Quarantine             | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             |
| Web URL Block          | <input type="checkbox"/>                                             |                                                                      |                                                                      |                                                                      |                                                                      |
| Web Content Block      | <input type="checkbox"/>                                             |                                                                      |                                                                      |                                                                      |                                                                      |
| Web Script Filter      | <input type="checkbox"/>                                             |                                                                      |                                                                      |                                                                      |                                                                      |
| Web Exempt List        | <input type="checkbox"/>                                             |                                                                      |                                                                      |                                                                      |                                                                      |
| Email Block List       |                                                                      |                                                                      | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             |                                                                      |
| Email Exempt List      |                                                                      |                                                                      | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             |                                                                      |
| Email Content Block    |                                                                      |                                                                      | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             |                                                                      |
| Oversized File/Email   | <input type="radio"/> block<br><input checked="" type="radio"/> pass | <input type="radio"/> block<br><input checked="" type="radio"/> pass | <input type="radio"/> block<br><input checked="" type="radio"/> pass | <input type="radio"/> block<br><input checked="" type="radio"/> pass | <input type="radio"/> block<br><input checked="" type="radio"/> pass |
| Pass Fragmented Emails |                                                                      |                                                                      | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             |

OK Cancel

## Adding a content profile to a policy

You can add content profiles to policies with action set to allow or encrypt and with Service set to ANY, HTTP, FTP, IMAP, POP3, SMTP, or a service group that includes these services.

- 1 Go to **Firewall > Policy**.
- 2 Select a policy list that contains policies to which to add a content profile.  
For example, to enable network protection for files downloaded by internal network users from the web, select an internal to external policy list.

- 3 Select New to add a new policy, or choose a policy and select Edit .
- 4 Select Anti-Virus & Web filter.
- 5 Select a content profile.
- 6 Configure the remaining policy settings if required.
- 7 Select OK.
- 8 Repeat this procedure for any policies for which to enable network protection.

# Users and authentication

FortiGate units support user authentication to the FortiGate user database, to a RADIUS server, and to an LDAP server. You can add user names to the FortiGate user database and then add a password to allow the user to authenticate using the internal database. You can also add the names of RADIUS and LDAP servers. You can select RADIUS to allow the user to authenticate using the selected RADIUS server or LDAP to allow the user to authenticate using the selected LDAP server. You can disable a user name so that the user cannot authenticate.

To enable authentication, you must add user names to one or more user groups. You can also add RADIUS servers and LDAP servers to user groups. You can then select a user group when you require authentication.

You can select user groups to require authentication for:

- any firewall policy with Action set to ACCEPT
- IPSec dialup user phase 1 configurations
- XAuth functionality for Phase 1 IPSec VPN configurations
- PPTP
- L2TP

When a user enters a user name and password, the FortiGate unit searches the internal user database for a matching user name. If Disable is selected for that user name, the user cannot authenticate and the connection is dropped. If Password is selected for that user and the password matches, the connection is allowed. If the password does not match, the connection is dropped.

If RADIUS is selected and RADIUS support is configured and the user name and password match a user name and password on the RADIUS server, the connection is allowed. If the user name and password do not match a user name and password on the RADIUS server, the connection is dropped.

If LDAP is selected and LDAP support is configured and the user name and password match a user name and password on the LDAP server, the connection is allowed. If the user name and password do not match a user name and password on the LDAP server, the connection is dropped.

If the user group contains user names, RADIUS servers, and LDAP servers, the FortiGate unit checks them in the order in which they have been added to the user group.

This chapter describes:

- [Setting authentication timeout](#)
- [Adding user names and configuring authentication](#)
- [Configuring RADIUS support](#)
- [Configuring LDAP support](#)
- [Configuring user groups](#)

## Setting authentication timeout

To set authentication timeout:

- 1 Go to **System > Config > Options**.
- 2 Set Auth Timeout to control how long authenticated firewall connections can remain idle before users must authenticate again to get access through the firewall.  
The default authentication timeout is 15 minutes.

## Adding user names and configuring authentication

Use the following procedures to add user names and configure authentication.

This section describes:

- [Adding user names and configuring authentication](#)
- [Deleting user names from the internal database](#)

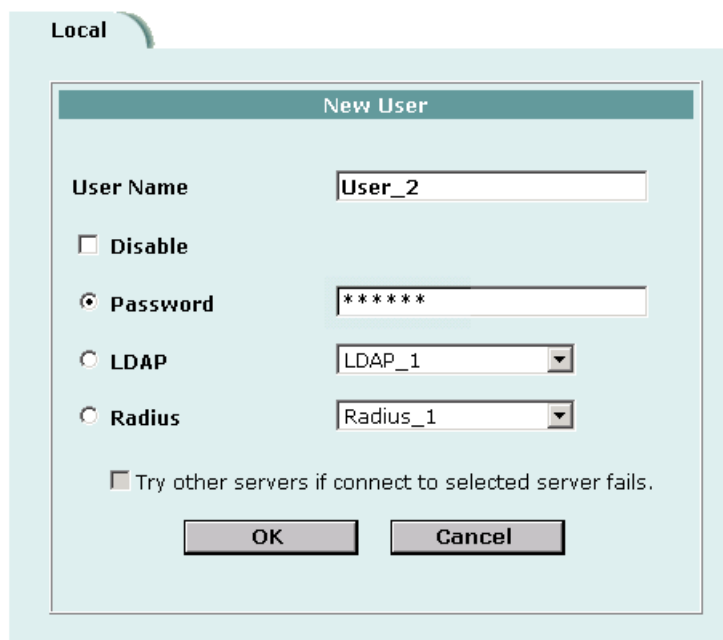
### Adding user names and configuring authentication

- 1 Go to **User > Local**.
- 2 Select New to add a new user name.
- 3 Enter the user name.  
The user name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.
- 4 Select one of the following authentication configurations:

|                 |                                                                                                                                                                                                                                                                                               |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Disable</b>  | Prevent this user from authenticating.                                                                                                                                                                                                                                                        |
| <b>Password</b> | Enter the password that this user must use to authenticate. The password should be at least six characters long. The password can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed. |
| <b>LDAP</b>     | Require the user to authenticate to an LDAP server. Select the name of the LDAP server to which the user must authenticate. You can only select an LDAP server that has been added to the FortiGate LDAP configuration. See <a href="#">"Configuring LDAP support" on page 177</a> .          |
| <b>Radius</b>   | Require the user to authenticate to a RADIUS server. Select the name of the RADIUS server to which the user must authenticate. You can only select a RADIUS server that has been added to the FortiGate RADIUS configuration. See <a href="#">"Configuring RADIUS support" on page 176</a> .  |

- 5 Select Try other servers if connect to selected server fails if you have selected Radius and you want the FortiGate unit to try to connect to other RADIUS servers added to the FortiGate RADIUS configuration.
- 6 Select OK.

Figure 17: Adding a user name



The screenshot shows a 'New User' dialog box within the 'Local' user management section. The dialog has a title bar 'New User'. It contains the following fields and options:

- User Name:** A text field containing 'User\_2'.
- Disable:** A checkbox that is unchecked.
- Password:** A text field with masked characters '\*\*\*\*\*'.
- LDAP:** A dropdown menu showing 'LDAP\_1'.
- Radius:** A dropdown menu showing 'Radius\_1'.
- Try other servers if connect to selected server fails:** A checkbox that is unchecked.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

## Deleting user names from the internal database

You cannot delete user names that have been added to user groups. Remove user names from user groups before deleting them

- 1 Go to **User > Local**.
- 2 Select Delete User  for the user name to delete.
- 3 Select OK.



**Note:** Deleting the user name deletes the authentication configured for the user.

## Configuring RADIUS support

If you have configured RADIUS support and a user is required to authenticate using a RADIUS server, the FortiGate unit contacts the RADIUS server for authentication.

This section describes:

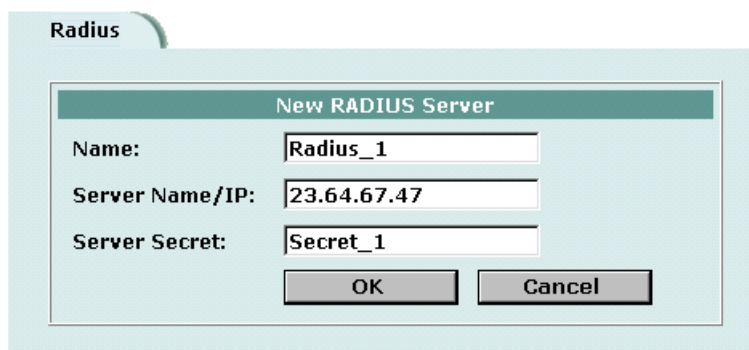
- [Adding RADIUS servers](#)
- [Deleting RADIUS servers](#)

### Adding RADIUS servers

To configure the FortiGate unit for RADIUS authentication:

- 1 Go to **User > RADIUS**.
- 2 Select New to add a new RADIUS server.
- 3 Enter the name of the RADIUS server.  
You can enter any name. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.
- 4 Enter the domain name or IP address of the RADIUS server.
- 5 Enter the RADIUS server secret.
- 6 Select OK.

Figure 18: Example RADIUS configuration



The screenshot shows a 'Radius' tab in the configuration interface. A 'New RADIUS Server' dialog box is open, containing the following fields and values:

| New RADIUS Server |             |
|-------------------|-------------|
| Name:             | Radius_1    |
| Server Name/IP:   | 23.64.67.47 |
| Server Secret:    | Secret_1    |

At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

### Deleting RADIUS servers

You cannot delete RADIUS servers that have been added to user groups.

- 1 Go to **User > RADIUS**.
- 2 Select Delete  beside the RADIUS server name that you want to delete.
- 3 Select OK.

## Configuring LDAP support

If you have configured LDAP support and a user is required to authenticate using an LDAP server, the FortiGate unit contacts the LDAP server for authentication. To authentication with the FortiGate unit, the user enters a user name and password. The FortiGate unit sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the user is successfully authenticated with the FortiGate unit. If the LDAP server cannot authenticate the user, the connection is refused by the FortiGate unit.

The FortiGate unit supports LDAP protocol functionality defined in RFC2251 for looking up and validating user names and passwords. FortiGate LDAP supports all LDAP servers compliant with LDAP v3.

FortiGate LDAP support does not extend to proprietary functionality, such as notification of password expiration, that is available from some LDAP servers. FortiGate LDAP support does not supply information to the user about why authentication failed.

LDAP user authentication is supported for PPTP, L2TP, IPsec VPN and firewall authentication. With PPTP, L2TP, and IPsec VPN, PAP (packet authentication protocol) is supported and CHAP (Challenge-Handshake Authentication Protocol) is not.

This section describes:

- [Adding LDAP servers](#)
- [Deleting LDAP servers](#)

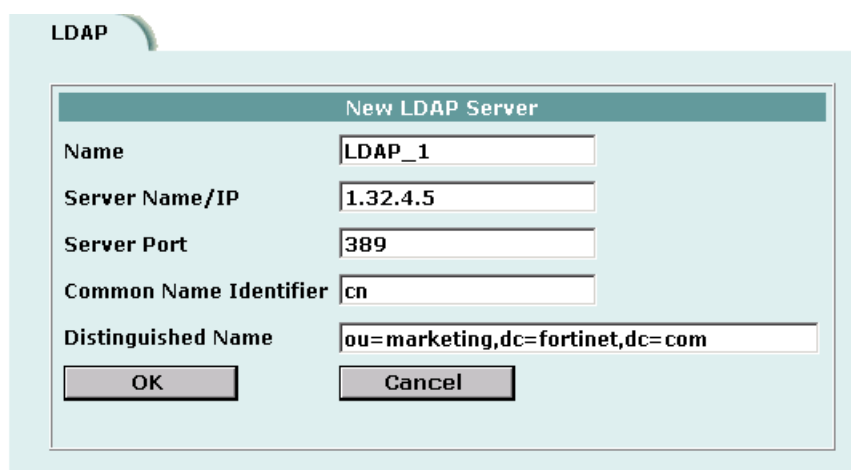
### Adding LDAP servers

To configure the FortiGate unit for LDAP authentication:

- 1 Go to **User > LDAP**.
- 2 Select New to add a new LDAP server.
- 3 Enter the name of the LDAP server.  
You can enter any name. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.
- 4 Enter the domain name or IP address of the LDAP server.
- 5 Enter the port used to communicate with the LDAP server.  
By default LDAP uses port 389.
- 6 Enter the common name identifier for the LDAP server.  
The common name identifier for most LDAP servers is cn. However some servers use other common name identifiers such as uid.

- 7 Enter the distinguished name used to look up entries on the LDAP server.  
Enter the base distinguished name for the server using the correct X.500 or LDAP format. The FortiGate unit passes this distinguished name unchanged to the server.  
For example, you could use the following base distinguished name:  
ou=marketing,dc=fortinet,dc=com  
where ou is organization unit and dc is domain component  
You can also specify multiple instances of the same field in the distinguished name, for example, to specify multiple organization units:  
ou=accounts,ou=marketing,dc=fortinet,dc=com
- 8 Select OK.

Figure 19: Example LDAP configuration



The screenshot shows a 'New LDAP Server' configuration window. It has a title bar with the text 'New LDAP Server' and a tab labeled 'LDAP'. The window contains five text input fields with the following values: 'Name' is 'LDAP\_1', 'Server Name/IP' is '1.32.4.5', 'Server Port' is '389', 'Common Name Identifier' is 'cn', and 'Distinguished Name' is 'ou=marketing,dc=fortinet,dc=com'. At the bottom of the window are two buttons: 'OK' and 'Cancel'.

## Deleting LDAP servers

You cannot delete LDAP servers that have been added to user groups.

- 1 Go to **User > LDAP**.
- 2 Select Delete  beside the LDAP server name that you want to delete.
- 3 Select OK.

## Configuring user groups

To enable authentication, you must add user names, RADIUS servers and LDAP servers to one or more user groups. You can then select a user group when you require authentication. You can select a user group to configure authentication for:

- Policies that require authentication. Only users in the selected user group or that can authenticate with the RADIUS servers added to the user group can authenticate with these policies.
- IPsec VPN Phase 1 configurations for dialup users. Only users in the selected user group can authenticate to use the VPN tunnel.
- XAuth for IPsec VPN Phase 1 configurations. Only users in the selected user group can be authenticated using XAuth.
- The FortiGate PPTP configuration. Only users in the selected user group can use PPTP.
- The FortiGate L2TP configuration. Only users in the selected user group can use L2TP.

When you add user names, RADIUS servers, and LDAP servers to a user group the order in which they are added affects the order in which the FortiGate unit checks for authentication. If user names are first, then the FortiGate unit checks for a match with these local users. If a match is not found, the FortiGate unit checks the RADIUS or LDAP server. If a RADIUS or LDAP server is added first, the FortiGate unit checks the server and then the local users.

If the user group contains users, RADIUS servers, and LDAP servers, the FortiGate unit checks them in the order in which they have been added to the user group.

This section describes:

- [Adding user groups](#)
- [Deleting user groups](#)

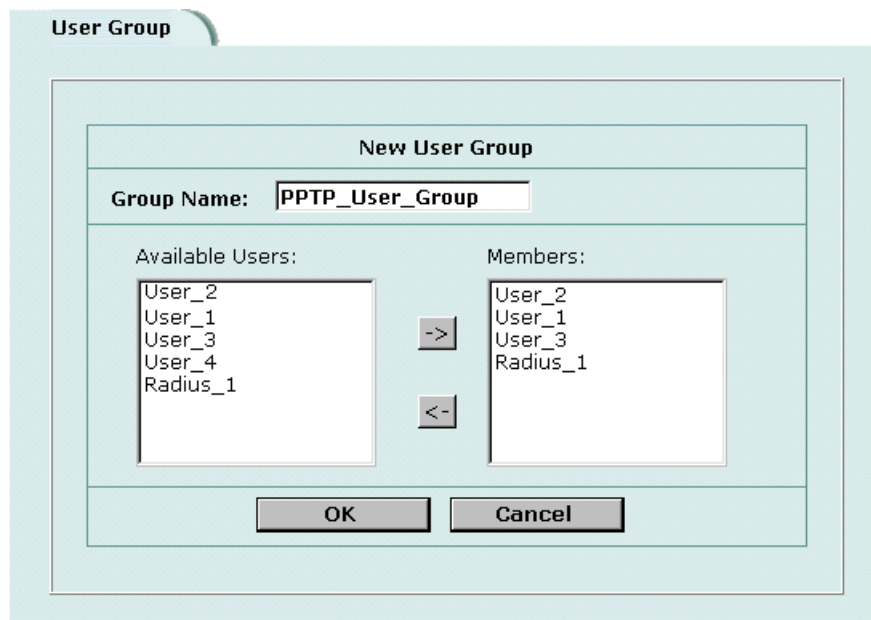
### Adding user groups

Use the following procedure to add user groups to the FortiGate configuration. You can add user names, RADIUS servers, and LDAP servers to user groups.

To add a user group:

- 1 Go to **User > User Group**.
- 2 Select New to add a new user group.

Figure 20: Adding a user group



- 3 Enter a Group Name to identify the user group.  
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.
- 4 To add users to the user group, select a user from the Available Users list and select the right arrow to add the name to the Members list.
- 5 To add a RADIUS server to the user group, select a RADIUS server from the Available Users list and select the right arrow to add the RADIUS server to the Members list.
- 6 To add an LDAP server to the user group, select an LDAP server from the Available Users list and select the right arrow to add the LDAP server to the Members list.
- 7 To remove users, RADIUS servers, or LDAP servers from the user group, select a user, RADIUS server, or LDAP server from the Members list and select the left arrow to remove the name, RADIUS server, or LDAP server from the group.
- 8 Select OK.

## Deleting user groups

You cannot delete user groups that have been selected in a policy, a dialup user phase1 configuration, or in a PPTP or L2TP configuration.

To delete a user group:

- 1 Go to **User > User Group**
- 2 Select Delete  beside the user group that you want to delete.
- 3 Select OK.

# IPSec VPN

A Virtual Private Network (VPN) is an extension of a private network that encompasses links across shared or public networks such as the Internet. For example, a company that has two offices in different cities, each with its own private network, can employ a VPN to create a secure tunnel between the offices. Similarly, a teleworker can use a VPN client to gain remote access to his private office network. In both cases, the secure connection appears to the user as a private network communication, even though the communication is carried over a public network.

Secure VPN connections are enabled by a combination of tunneling, data encryption and authentication. Tunneling encapsulates data so that it can be transferred over the public network. Instead of being sent in its original format, the data frames are encapsulated within an additional header and then routed between tunnel endpoints. Upon arrival at the destination endpoint, the data is decapsulated and forwarded to its destination within the private network.

Encryption transforms data stream from clear text (something that a human or a program can interpret) to cipher text (something that cannot be interpreted). The information is encrypted and decrypted using mathematical algorithms known as keys.

Authentication provides a means to verify the origin of a packet and the integrity of its contents. Authentication is completed using checksums calculated with keyed hash function algorithms.

This chapter provides an overview of how to configure FortiGate IPSec VPN. For a complete description of FortiGate VPN, see the *FortiGate VPN Guide*.

- [Key management](#)
- [Manual key IPSec VPNs](#)
- [AutoIKE IPSec VPNs](#)
- [Managing digital certificates](#)
- [Configuring encrypt policies](#)
- [IPSec VPN concentrators](#)
- [Redundant IPSec VPNs](#)
- [Monitoring and Troubleshooting VPNs](#)

## Key management

There are three basic elements in any encryption system:

- an algorithm which changes information into code,
- a cryptographic key which serves as a secret starting point for the algorithm,
- a management system to control the key.

IPSec provides two ways to handle key exchange and management: manual keying and IKE for automated key management.

- [Manual Keys](#)
- [Automatic Internet Key Exchange \(AutoIKE\) with pre-shared keys or certificates](#)

### Manual Keys

When manual keys are employed, matching security parameters must be entered at both ends of the tunnel. These settings, which include both the encryption and authentication keys, must be kept secret so that unauthorized parties cannot decrypt the data, even if they know which encryption algorithm is being used.

### Automatic Internet Key Exchange (AutoIKE) with pre-shared keys or certificates

To facilitate deployment of multiple tunnels, an automated system of key management is required. IPSec supports the automated generation and negotiation of keys using the Internet Key Exchange protocol. This method of key management is typically referred to as AutoIKE. Fortinet supports AutoIKE with pre-shared keys and AutoIKE with certificates.

#### AutoIKE with pre-shared keys

When both peers in a session have been configured with the same pre-shared key, they can use it to authenticate themselves to each other. The peers do not actually send the key to each other. Instead, as part of the security negotiation process, they use it in combination with a Diffie-Hellman group to create a session key. The session key is used for encryption and authentication purposes, and is automatically regenerated during the communication session by IKE.

Pre-shared keys are similar to the manual keys in that they require the network administrator to distribute and manage matching information at the VPN peer sites. Whenever a pre-shared key changes, the administrator must update both sites.

#### AutoIKE with certificates

This method of key management involves the participation of a trusted third party, the certificate authority (CA). Each peer in a VPN is first required to generate a set of keys, known as a public/private key pair. The CA signs the public key for each peer, creating a signed digital certificate. The peer then contacts the CA to retrieve their own certificates, plus that of the CA itself. Once the certificates have been uploaded to the FortiGate units and appropriate IPSec tunnels and policies have been configured, the peers are ready to start communicating. As they do, IKE manages the exchange of certificates, transmitting signed digital certificates from one peer to another. The signed digital certificates are validated by the presence of the CA certificate at each end. With authentication complete, the IPSec tunnel is then established.

In some respects, certificates are simpler to manage than manual keys or pre-shared keys. For this reason, certificates are best suited to large network deployments.

## Manual key IPSec VPNs

When manual keys are employed, complementary security parameters must be entered at both ends of the tunnel. In addition to encryption and authentication algorithms and keys, the security parameter index (SPI) is required. The SPI is an arbitrary value that defines the structure of the communication between the peers. With other methods the SPI is generated automatically but with the manual key configuration it must be entered as part of the VPN setup.

The encryption and authentication keys must match on the local and remote peers; the SPI values must be mirror images of each other. After you enter these values, the VPN tunnel can start without any need for the authentication and encryption algorithms to be negotiated. So long as you have entered correct, complementary values, the tunnel will be established between the peers. In essence, the tunnel already exists between the peers. As a result, when traffic matches a policy requiring the tunnel, it can be authenticated and encrypted immediately.

- [General configuration steps for a manual key VPN](#)
- [Adding a manual key VPN tunnel](#)

### General configuration steps for a manual key VPN

A manual key VPN configuration consists of a manual key VPN tunnel, the source and destination addresses for both ends of the tunnel, and an encrypt policy to control access to the VPN tunnel.

To create a manual key VPN configuration:

- 1 Add a manual key VPN tunnel. See [“Adding a manual key VPN tunnel” on page 183](#).
- 2 Configure an encrypt policy that includes the tunnel, source address, and destination address for both ends of the tunnel. See [“Configuring encrypt policies” on page 196](#).

### Adding a manual key VPN tunnel

Configure a manual key tunnel to create an IPSec VPN tunnel between the FortiGate unit and a remote IPSec VPN client or gateway that is also using manual key.

To add a manual key VPN tunnel:

To add a manual key VPN tunnel:

- 1 Go to **VPN > IPSec > Manual Key**.
- 2 Select New to add a new manual key VPN tunnel.
- 3 Enter a VPN Tunnel Name.  
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.
- 4 Enter the Local SPI.  
The Local Security Parameter Index is a hexadecimal number of up to eight digits (digits can be 0 to 9, a to f) in the range bb8 to FFFFFFFF. This number must be added to the Remote SPI at the opposite end of the tunnel.

- 5 Enter the Remote SPI.  
The Remote Security Parameter Index is a hexadecimal number of up to eight digits (digits can be 0 to 9, a to f) in the range bb8 to FFFFFFFF. This number must be added to the Local SPI at the opposite end of the tunnel.
- 6 Enter the Remote Gateway.  
This is the external IP address of the FortiGate unit or other IPSec gateway at the opposite end of the tunnel.
- 7 Select an Encryption Algorithm from the list.  
Use the same algorithm at both ends of the tunnel.
- 8 Enter the Encryption Key.  
Each two character combination entered in hexadecimal format represents one byte. Depending on the encryption algorithm you have selected, you may be required to enter the key in multiple segments. Use the same encryption key at both ends of the tunnel.  
  

|               |                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>DES</b>    | Enter a 16 character (8 byte) hexadecimal number (0-9, A-F).                                                            |
| <b>3DES</b>   | Enter a 48 character (24 byte) hexadecimal number (0-9, A-F). Separate the number into three segments of 16 characters. |
| <b>AES128</b> | Enter a 32 character (16 byte) hexadecimal number (0-9, A-F). Separate the number into two segments of 16 characters.   |
| <b>AES192</b> | Enter a 48 character (24 byte) hexadecimal number (0-9, A-F). Separate the number into three segments of 16 characters. |
| <b>AES256</b> | Enter a 64 character (32 byte) hexadecimal number (0-9, A-F). Separate the number into four segments of 16 characters.  |
- 9 Select an Authentication Algorithm from the list.  
Use the same algorithm at both ends of the tunnel.
- 10 Enter the Authentication Key.  
Each two character combination entered in hexadecimal format represents one byte. Use the same authentication key at both ends of the tunnel.  
  

|             |                                                                                                                                                              |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MD5</b>  | Enter a 32 character (16 byte) hexadecimal number (0-9, A-F). Separate the number into two segments of 16 characters.                                        |
| <b>SHA1</b> | Enter a 40 character (20 byte) hexadecimal number (0-9, A-F). Separate the number into two segments—the first of 16 characters; the second of 24 characters. |
- 11 Select a concentrator if you want the tunnel to be part of a hub and spoke VPN configuration. See [“Adding a VPN concentrator” on page 201](#).  
Select OK to save the manual key VPN tunnel.

## AutoIKE IPSec VPNs

FortiGate supports two methods of Automatic Internet Key Exchange (AutoIKE) for the purpose of establishing IPSec VPN tunnels: AutoIKE with pre-shared keys and AutoIKE with digital certificates.

- [General configuration steps for an AutoIKE VPN](#)
- [Adding a phase 1 configuration for an AutoIKE VPN](#)
- [Adding a phase 2 configuration for an AutoIKE VPN](#)

### General configuration steps for an AutoIKE VPN

An AutoIKE VPN configuration consists of phase 1 and phase 2 configuration parameters, the source and destination addresses for both ends of the tunnel, and an encrypt policy to control access to the VPN tunnel.

To create an AutoIKE VPN configuration:



**Note:** Prior to configuring an AutoIKE VPN that uses digital certificates, you must add the CA and local certificates to the FortiGate unit. For details, see [“Managing digital certificates” on page 191](#).

- 1 Add the phase 1 parameters. See [“Adding a phase 1 configuration for an AutoIKE VPN” on page 185](#).
- 2 Add the phase 2 parameters. See [“Adding a phase 2 configuration for an AutoIKE VPN” on page 189](#).
- 3 Configure an encrypt policy that includes the tunnel, source address, and destination address for both ends of the tunnel. See [“Configuring encrypt policies” on page 196](#).

### Adding a phase 1 configuration for an AutoIKE VPN

When you add a phase 1 configuration, you define the terms by which the FortiGate unit and a remote VPN peer (gateway or client) authenticate themselves to each other prior to the establishment of an IPSec VPN tunnel.

The phase 1 configuration is related to the phase 2 configuration. In phase 1 the VPN peers are authenticated; in phase 2 the tunnel is established. You have the option to use the same phase 1 parameters to establish multiple tunnels. In other words, the same remote VPN peer (gateway or client) can have multiple tunnels to the local VPN peer (the FortiGate unit).

When the FortiGate unit receives an IPSec VPN connection request, it authenticates the VPN peers according to the phase 1 parameters. Then, depending on the source and destination addresses of the request, it starts an IPSec VPN tunnel and applies an encrypt policy.

To add a phase 1 configuration:

- 1 Go to **VPN > IPSEC > Phase 1**.
- 2 Select New to add a new phase 1 configuration.

- 3 Enter a Gateway Name for the remote VPN peer.  
The remote VPN peer can be either a gateway to another network or an individual client on the Internet.  
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.
- 4 Select a Remote Gateway address type.
  - If the remote VPN peer has a static IP address, select Static IP Address.
  - If the remote VPN peer has a dynamically assigned IP address (DHCP or PPPoE), or if the remote VPN peer has a static IP address that is not required in the peer identification process, select Dialup User.
 Depending upon the Remote Gateway address type you have selected, other fields become available.

#### Remote Gateway: Static IP Address

**IP Address** If you select Static IP Address, the IP Address field appears. Enter the IP address of the remote IPSec VPN gateway or client that can connect to the FortiGate unit. This is a mandatory entry.

#### Remote Gateway: Dialup User

**Peer Options** If you select Dialup User, the Peer Options become available under Advanced Options. Use the Peer Options to authenticate remote VPN peers with peer IDs during phase 1 negotiations. For details, see [step 2](#).

- 5 Select Aggressive or Main (ID Protection) mode.  
When using aggressive mode, the VPN peers exchange identifying information in the clear. When using main mode, identifying information is hidden.  
The VPN peers must use the same mode.
- 6 Configure the P1 Proposal.  
Select up to three encryption and authentication algorithm combinations to propose for phase 1.  
The VPN peers must use the same P1 proposal settings.
- 7 Select the DH Group(s).  
Select one or more Diffie-Hellman groups to propose for phase 1.  
As a general rule, the VPN peers should use the same DH Group settings.
- 8 Enter the Keylife.  
The keylife is the amount of time in seconds before the phase 1 encryption key expires. When the key expires, a new key is generated without interrupting service. P1 proposal keylife can be from 120 to 172,800 seconds.
- 9 For Authentication Method, select Preshared Key or RSA Signature.
  - If you select Preshared key, enter a that is shared by the VPN peers. The key must contain at least 6 printable characters and should only be known by network administrators. To protect against the best-known attacks, a good pre-shared key should consist of a minimum of 16 randomly chosen alpha-numeric characters.
  - If you select RSA Signature, select a local certificate that has been digitally signed by the certificate authority (CA). To add a local certificate to the FortiGate unit, see [“Obtaining a signed local certificate” on page 191](#).

- 10** Optionally, enter the Local ID of the FortiGate unit.  
The entry is required if the FortiGate unit is functioning as a client and uses its local ID to authenticate itself to the remote VPN peer. (If you do not add a local ID, the FortiGate unit will transmit its IP address.)  
Configure the local ID only with pre-shared keys and aggressive mode. Do not configure the local ID with certificates or main mode.

### Configuring advanced options

- 1** Select Advanced Options.  
**2** Optionally, select a Peer Option.  
Use the Peer Options to authenticate remote VPN peers by the ID that they transmit during phase 1.

|                                       |                                                                                                                                                                                                                     |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Accept any peer ID</b>             | Select to accept any peer ID (and therefore not authenticate remote VPN peers by peer ID).                                                                                                                          |
| <b>Accept this peer ID</b>            | Select to authenticate a specific VPN peer or a group of VPN peers with a shared user name (ID) and password (pre-shared key). Also add the peer ID. Also add the peer ID.                                          |
| <b>Accept peer ID in dialup group</b> | Select to authenticate each remote VPN peer with a unique user name (ID) and password (pre-shared key). Also select a dialup group (user group).<br>Configure the user group prior to configuring this peer option. |

- 3** Optionally, configure XAuth.  
XAuth (IKE eXtended Authentication) authenticates VPN peers at the user level. If the the FortiGate unit (the local VPN peer) is configured as an XAuth server, it will authenticate remote VPN peers by referring to a user group. The users contained in the user group can be configured locally on the FortiGate unit or on remotely located LDAP or RADIUS servers. If the FortiGate unit is configured as an XAuth client, it will provide a user name and password when it is challenged.

#### XAuth: Enable as a Client

|                 |                                                                                            |
|-----------------|--------------------------------------------------------------------------------------------|
| <b>Name</b>     | Enter the user name the local VPN peer uses to authenticate itself to the remote VPN peer. |
| <b>Password</b> | Enter the password the local VPN peer uses to authenticate itself to the remote VPN peer.  |

#### XAuth: Enable as a Server

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Encryption method</b> | Select the encryption method used between the XAuth client, the FortiGate unit and the authentication server.<br><b>PAP</b> — Password Authentication Protocol.<br><b>CHAP</b> —Challenge-Handshake Authentication Protocol.<br><b>MIXED</b> —Select MIXED to use PAP between the XAuth client and the FortiGate unit, and CHAP between the FortiGate unit and the authentication server.<br>Use CHAP whenever possible. Use PAP if the authentication server does not support CHAP. (Use PAP with all implementations of LDAP and some implementations of Microsoft RADIUS). Use MIXED if the authentication server supports CHAP but the XAuth client does not. (Use MIXED with the Fortinet Remote VPN Client.). |
| <b>Usergroup</b>         | Select a group of users to be authenticated by XAuth. The individual users within the group can be authenticated locally or by one or more LDAP or RADIUS servers.<br>The user group must be added to the FortiGate configuration before it can be selected here.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

**4** Optionally, configure NAT Traversal.

|                            |                                                                                                                                                                                                                                                                                                                                               |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable</b>              | Select Enable if you expect the IPSec VPN traffic to go through a gateway that performs NAT. If no NAT device is detected, enabling NAT traversal will have no effect. Both ends of the VPN (both VPN peers) must have the same NAT traversal setting.                                                                                        |
| <b>Keepalive Frequency</b> | If you enable NAT-traversal, you can change the number of seconds in the Keepalive Frequency field. This number specifies, in seconds, how frequently empty UDP packets are sent through the NAT device to ensure that the NAT mapping does not change until P1 and P2 keylife expires. The keepalive frequency can be from 0 to 900 seconds. |

**5** Optionally, configure Dead Peer Detection.

Use these settings to monitor the status of the connection between VPN peers. DPD allows dead connections to be cleaned up and new VPN tunnels established. DPD is not supported by all vendors.

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable</b>         | Select Enable to enable DPD between the local and remote peers.                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Short Idle</b>     | Set the time, in seconds, that a link must remain unused before the local VPN peer considers it to be idle. After this period of time expires, whenever the local peer sends traffic to the remote VPN peer it will also send a DPD probe to determine the status of the link. To control the length of time that the FortiGate unit takes to detect a dead peer with DPD probes, configure the Retry Count and the Retry Interval. |
| <b>Retry Count</b>    | Set the number of times that the local VPN peer will retry the DPD probe before it considers the channel to be dead and tears down the security association (SA). To avoid false negatives due to congestion or other transient failures, set the retry count to a sufficiently high value for your network.                                                                                                                        |
| <b>Retry Interval</b> | Set the time, in seconds, that the local VPN peer unit waits between retrying DPD probes.                                                                                                                                                                                                                                                                                                                                           |
| <b>Long Idle</b>      | Set the period of time, in seconds, that a link must remain unused before the local VPN peer pro-actively probes its state. After this period of time expires, the local peer will send a DPD probe to determine the status of the link even if there is no traffic between the local peer and the remote peer.                                                                                                                     |

**6** Select OK to save the phase 1 parameters.

Figure 21: Adding a phase 1 configuration

The screenshot shows the 'New VPN Gateway' configuration window. The 'Gateway Name' is 'Remote\_Client\_2'. The 'Remote Gateway' is set to 'Static IP Address' with the IP '2.2.2.2'. The 'Mode' is 'Main (ID protection)'. The 'P1 Proposal' has two entries: '1 - Encryption: 3DES, Authentication: SHA1' and '2 - Encryption: 3DES, Authentication: MD5'. The 'DH Group' is '2'. The 'Keylife' is '28800' seconds. The 'Authentication Method' is 'Preshared Key'. The 'Pre-shared Key' is masked with asterisks. The 'Local ID' is optional. The 'Advanced Options' are checked, including 'Accept any peer ID', 'XAuth' (disabled), 'Nat-traversal' (enabled), 'Keepalive Frequency' (5 seconds), and 'Dead Peer Detection' (enabled with a 10-second short idle, 3 retries, 5-second interval, and 300-second long idle). The 'OK' and 'Cancel' buttons are at the bottom.

## Adding a phase 2 configuration for an AutoIKE VPN

Add a phase 2 configuration to specify the parameters used to create and maintain a VPN tunnel between the local VPN peer (the FortiGate unit) and the remote VPN peer (the VPN gateway or client).



**Note:** Adding a Phase 2 configuration is the same for pre-shared key and certification VPNs.

To add a phase 2 configuration:

- 1 Go to **VPN > IPSEC > Phase 2**.
- 2 Select **New** to add a new phase 2 configuration.
- 3 Enter a Tunnel Name.

The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.

- 4 Select a Remote Gateway to associate with the VPN tunnel.  
A remote gateway can be either a gateway to another network or an individual client on the Internet. Remote gateways are added as part of the phase 1 configuration. For details, see [“Adding a phase 1 configuration for an AutoIKE VPN” on page 185](#).  
Choose either a single DIALUP remote gateway, or up to three STATIC remote gateways. Multiple STATIC remote gateways are necessary if you are configuring IPSec redundancy. For information about IPSec redundancy, see [“Redundant IPSec VPNs” on page 203](#).
- 5 Configure the P2 Proposal.  
Select up to three encryption and authentication algorithm combinations to propose for phase 2.  
The VPN peers must use the same P2 proposal settings.
- 6 Optionally, enable Replay Detection.  
Replay detection protects the VPN tunnel from replay attacks.



**Note:** Do not select replay detection if you have also selected Null Authentication for the P2 Proposal.

- 7 Optionally, enable Perfect Forward Secrecy (PFS).  
PFS improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.
- 8 Select the DH Group(s).  
The VPN peers must use the same DH Group settings.
- 9 Enter the Keylife.  
The keylife causes the phase 2 key to expire after a specified amount of time, after a specified number of kbytes of data have been processed by the VPN tunnel, or both. If you select both, the key does not expire until both the time has passed and the number of kbytes have been processed.  
When the key expires, a new key is generated without interrupting service. P2 proposal keylife can be from 120 to 172800 seconds or from 5120 to 99999 kbytes.
- 10 Optionally, enable Autokey Keep Alive.  
Enable Autokey Keep Alive to keep the VPN tunnel running even if no data is being processed.
- 11 Optionally, select a concentrator.  
Select a concentrator if you want the tunnel to be part of a hub and spoke VPN configuration. If you use the procedure, [“Adding a VPN concentrator” on page 201](#) to add the tunnel to a concentrator, the next time you open the tunnel, the Concentrator field displays the name of the concentrator to which you have added the tunnel.
- 12 Select OK to save the AutoIKE key VPN tunnel.

Figure 22: Adding a phase 2 configuration

The screenshot shows the 'New VPN Tunnel' configuration window in the FortiGate GUI. The 'Phase 2' tab is active. The 'Tunnel Name' is 'Tunnel\_1' and the 'Remote Gateway' is 'Remote\_Client\_1'. Under 'P2 Proposal', there are three proposals: 1-Encryption: 3DES, Authentication: SHA1; 2-Encryption: 3DES, Authentication: MD5; 3-Encryption: AES128, Authentication: MD5. The 'Enable replay detection' and 'Enable perfect forward secrecy(PFS)' checkboxes are checked. The 'DH Group' is set to 5. The 'Keylife' is set to 1800 seconds and 4608000 KBytes. The 'Autokey Keep Alive' checkbox is unchecked. The 'Concentrator' is set to 'None'. 'OK' and 'Cancel' buttons are at the bottom.

## Managing digital certificates

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants.

Fortinet uses a manual procedure to obtain certificates. This involves copying and pasting text files from your local computer to the certificate authority, and from the certificate authority to your local computer.

- [Obtaining a signed local certificate](#)
- [Obtaining a CA certificate](#)



**Note:** Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

### Obtaining a signed local certificate

The signed local certificate provides the FortiGate unit with a means to authenticate itself to other devices.



**Note:** The VPN peers must use digital certificates that adhere to the X.509 standard.

## Generating the certificate request

With this procedure, you generate a private and public key pair. The public key is the base component of the certificate request.

To generate the certificate request:

- 1 Go to **VPN > Local Certificates**.

- 2 Select **Generate**.

- 3 Enter a **Certificate Name**.

The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.

- 4 Configure the **Subject Information** that identifies the object being certified.

Preferably use an IP address or domain name. If this is impossible (such as with a dialup client), use an e-mail address.

|                    |                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Host IP</b>     | For Host IP, enter the IP address of the FortiGate unit being certified.                                                                                                            |
| <b>Domain Name</b> | For Domain name, enter the fully qualified domain name of the FortiGate unit being certified. Do not include the protocol specification (http://) or any port number or path names. |
| <b>E-Mail</b>      | For E-mail, enter the email address of the owner of the FortiGate unit being certified. Typically, e-mail addresses are entered only for clients, not gateways.                     |

- 5 Configure the **Optional Information** to further identify the object being certified.

|                          |                                                                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Organization Unit</b> | Enter a name that identifies the department or unit within the organization that is requesting the certificate for the FortiGate unit (such as Manufacturing or MF). |
| <b>Organization</b>      | Enter the legal name of the organization that is requesting the certificate for the FortiGate unit (such as Fortinet).                                               |
| <b>Locality</b>          | Enter the name of the city or town where the FortiGate unit is located (such as Vancouver).                                                                          |
| <b>State/Province</b>    | Enter the name of the state or province where the FortiGate unit is located (such as California or CA).                                                              |
| <b>Country</b>           | Select the country where the FortiGate unit is located.                                                                                                              |
| <b>e-mail</b>            | Enter a contact e-mail address for the FortiGate unit. Typically, e-mail addresses are entered only for clients, not gateways.                                       |

- 6 Configure the key.

|                 |                                                                                                                                          |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Key Type</b> | Select RSA as the key encryption type. No other key type is supported.                                                                   |
| <b>Key Size</b> | Select 1024 Bit, 1536 Bit or 2048 Bit. Larger keys are slower to generate but more secure. Not all products support all three key sizes. |

- 7 Select **OK** to generate the private and public key pair and the certificate request.

The private/public key pair will be generated and the certificate request will be displayed on the Local Certificates list with a status of Pending.

**Figure 23: Adding a Local Certificate**

The screenshot shows the 'Local Certificates' configuration page. The main heading is 'Local Certificates'. Below it is a section titled 'Generate Certificate Signing Request'. The form contains the following fields:

- Certification Name:** User\_One
- Subject Information:**
  - ID Type: E-Mail (dropdown)
  - e-mail: one@fortinet.com
- Optional Information:**
  - Organization Unit: MF
  - Organization: Fortinet
  - Locality(City): Vancouver
  - State/Province: BC
  - Country: CANADA (dropdown)
  - e-mail: (empty field)
- Key Type:** RSA (dropdown)
- Key Size:** 1024 Bit (dropdown)

At the bottom of the form are two buttons: 'OK' and 'Cancel'.

### Downloading the certificate request

With this procedure, you download the certificate request from the FortiGate unit to the management computer.

To download the certificate request:

- 1 Go to **VPN > Local Certificates**.
- 2 Select Download  to download the local certificate to the management computer.
- 3 Select Save.
- 4 Name the file and save it in a directory on the management computer.

### Requesting the signed local certificate

With this procedure, you copy and paste the certificate request from the management computer to the CA web server.

To request the signed local certificate:

- 1 On the management computer, open the local certificate request in a text editor.
- 2 Copy the certificate request.
- 3 Connect the CA web server.

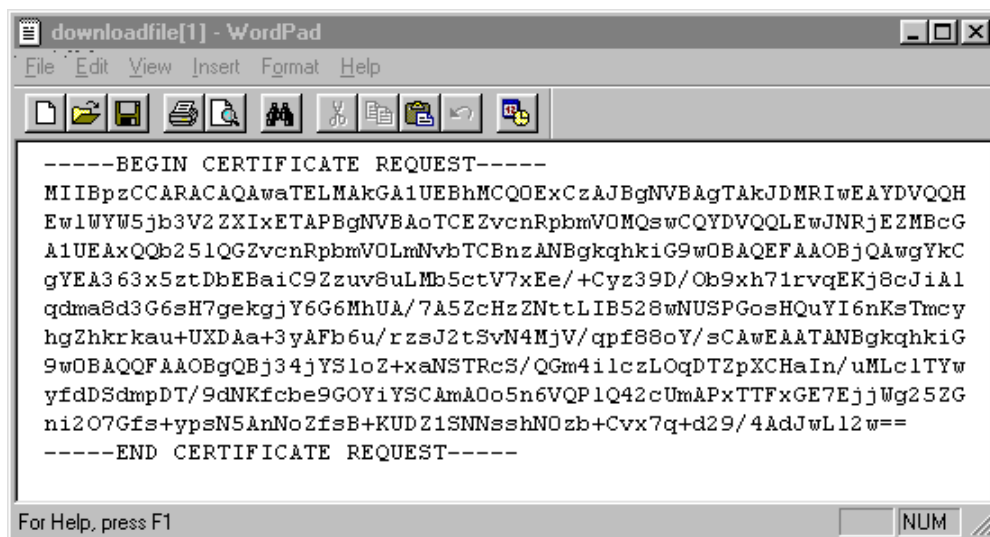
#### 4 Request the signed local certificate.

Follow the CA web server instructions to:

- add a base64 encoded PKCS#10 certificate request to the CA web server,
- paste the certificate request to the CA web server,
- submit the certificate request to the CA web server.

The certificate request is submitted to the CA for it to sign.

**Figure 24: Opening a certificate request in a text editor**



### Retrieving the signed local certificate

With this procedure, you connect to the CA web server and download the signed local certificate to the management computer. (Do this after receiving notification from the CA that it has signed the certificate request.)

To retrieve the signed local certificate:

- 1 Connect the CA web server.
- 2 Follow the CA web server instructions to download the signed local certificate.

The File Download dialog will display.

- 3 Select Save.
- 4 Save the file in a directory on the management computer.

### Importing the signed local certificate

With this procedure, you import the signed local certificate from the management computer to the FortiGate unit.

To import the signed local certificate:

- 1 Go to **VPN > Local Certificates**.
- 2 Select Import.

- 3 Enter the path or browse to locate the signed local certificate on the management computer.
- 4 Select OK.  
The signed local certificate will be displayed on the Local Certificates list with a status of OK.

## Obtaining a CA certificate

For the VPN peers to authenticate themselves to each other, they must both obtain a CA certificate from the same certificate authority. The CA certificate provides the VPN peers with a means to validate the digital certificates that they receive from other devices.

The FortiGate unit obtains the CA certificate in order to validate the digital certificate that it receives from the remote VPN peer. The remote VPN peer obtains the CA certificate in order to validate the digital certificate that it receives from the FortiGate unit.



**Note:** The CA certificate must adhere to the X.509 standard.

## Retrieving a CA certificate

Connect to the CA web server and download the CA certificate to the management computer.

To retrieve the CA certificate:

- 1 Connect the CA web server.
- 2 Follow the CA web server instructions to download the CA certificate.  
The File Download dialog will display.
- 3 Select Save.
- 4 Save the CA certificate in a directory on the management computer.

## Importing a CA certificate

Import the signed local certificate from the management computer to the FortiGate unit.

To import the CA certificate:

- 1 Go to **VPN > CA Certificates**.
- 2 Select Import.
- 3 Enter the path or browse to locate the CA certificate on the management computer.
- 4 Select OK.  
The CA will be displayed on the CA Certificates list.

## Configuring encrypt policies

A VPN connects the local, internal network to a remote, external network. The principal role of the encrypt policy is to define (and limit) which addresses on these networks can use the VPN.

A VPN requires only one encrypt policy to control both inbound and outbound connections. Depending on how you configure it, the policy controls whether users on your internal network can establish a tunnel to the remote network (the outbound connection), and whether users on the remote network can establish a tunnel to your internal network (the inbound connection). This flexibility allows a single encrypt policy to do the job of two regular firewall policies.

Although the encrypt policy controls both incoming and outgoing connections, it must always be configured as an outgoing policy. An outgoing policy has a source address on an internal network and a destination address on an external network. The source address identifies which addresses on the internal network are part of the VPN. The destination address identifies which addresses on the remote network are part of the VPN. Typical outgoing policies include Internal-to-External and DMZ-to-External.



**Note:** The destination address can be a VPN client address on the Internet or the address of a network behind a remote VPN gateway.

In addition to defining membership in the VPN by address, you can configure the encrypt policy for services such as DNS, FTP, and POP3, and to allow connections according to a predefined schedule (by the time of the day or the day of the week, month, or year). You can also configure the encrypt policy for:

- Inbound NAT to translate the source of incoming packets.
- Outbound NAT to translate the source address of outgoing packets.
- Traffic shaping to control the bandwidth available to the VPN and the priority of the VPN.
- Content profiles to apply antivirus protection, web filtering, and email filtering to web, file transfer, and email services in the VPN.
- Logging so that the FortiGate unit logs all connections that use the VPN.

The policy must also include the VPN tunnel that you created to communicate with the remote FortiGate VPN gateway. When users on your internal network attempt to connect to the network behind the remote VPN gateway, the encrypt policy intercepts the connection attempt and starts the VPN tunnel added to the policy. The tunnel uses the remote gateway added to its configuration to connect to the remote VPN gateway. When the remote VPN gateway receives the connection attempt, it checks its own policy, gateway and tunnel configuration. If the configuration is allowed, an IPSec VPN tunnel is negotiated between the two VPN peers.

- [Adding a source address](#)
- [Adding a destination address](#)
- [Adding an encrypt policy](#)

## Adding a source address

The source address is located within the internal network of the local VPN peer. It can be a single computer address or the address of a network.

- 1 Go to **Firewall > Address**.
- 2 Select an internal interface. (Methods will differ slightly between FortiGate models.)
- 3 Select New to add an address.
- 4 Enter the Address Name, IP Address, and NetMask for a single computer or for an entire subnetwork on an internal interface of the local VPN peer.
- 5 Select OK to save the source address.

## Adding a destination address

The destination address can be a VPN client address on the Internet or the address of a network behind a remote VPN gateway.

- 1 Go to **Firewall > Address**.
- 2 Select an external interface. (Methods will differ slightly between FortiGate models.)
- 3 Select New to add an address.
- 4 Enter the Address Name, IP Address, and NetMask for a single computer or for an entire subnetwork on an internal interface of the remote VPN peer.
- 5 Select OK to save the source address.

## Adding an encrypt policy

- 1 Go to **Firewall > Policy**.
- 2 Select the policy list to which you want to add the policy.  
For example, Int->Ext or DMZ->Ext.
- 3 Select New to add a new policy.
- 4 Set Source to the source address.
- 5 Set Destination to the destination address.
- 6 Set Service to control the services allowed over the VPN connection.  
You can select ANY to allow all supported services over the VPN connection or select a specific service or service group to limit the services allowed over the VPN connection.
- 7 Set Action to ENCRYPT.
- 8 Configure the ENCRYPT parameters.

**VPN Tunnel** Select an Auto Key tunnel for this encrypt policy.

**Allow inbound** Select Allow inbound to enable inbound users to connect to the source address.

**Allow outbound** Select Allow outbound to enable outbound users to connect to the destination address.

- Inbound NAT** The FortiGate unit translates the source address of incoming packets to the IP address of the FortiGate interface connected to the source address network. Typically, this is an internal interface of the FortiGate unit. Inbound NAT makes it impossible for local hosts to see the IP addresses of remote hosts (hosts located on the network behind the remote VPN gateway).
- Outbound NAT** The FortiGate unit translates the source address of outgoing packets to the IP address of the FortiGate interface connected to the destination address network. Typically, this is an external interface of the FortiGate unit. Outbound NAT makes it impossible for remote hosts to see the IP addresses of local hosts (hosts located on the network behind the local VPN gateway). If Outbound NAT is implemented, it is subject to these limitations:
- Configure Outbound NAT only at one end of the tunnel.
  - The end which does not implement Outbound NAT requires an Int->Ext policy which specifies the other end's external interface as the Destination. (This will be a public IP address.)
  - The tunnel, and the traffic within the tunnel, can only be initiated at the end which implements Outbound NAT.

Refer to the *FortiGate Installation and Configuration Guide* to configure the remaining policy settings.

9 Select OK to save the encrypt policy.

To make sure that the encrypt policy is matched for VPN connections, arrange the encrypt policy above other policies with similar source and destination addresses and services in the policy list.

**Figure 25: Adding an encrypt policy**

The screenshot displays the 'Edit Policy' configuration window in FortiGate. At the top, there are tabs for different traffic directions: Int->Ext, Int->DMZ, DMZ->Int, DMZ->Ext, Ext->Int, and Ext->DMZ. The 'Int->Ext' tab is selected. The main configuration area includes the following fields and options:

- Source:** FGT-100
- Destination:** FGT\_60
- Schedule:** Always
- Service:** ANY
- Action:** ENCRYPT
- VPN Tunnel:** FGT-60
- Allow inbound:** ☒
- Allow outbound:** ☒
- Inbound NAT:** ☐
- Outbound NAT:** ☐
- Traffic Shaping:** ☐
  - Guaranteed Bandwidth: 0 (KBytes/s)
  - Maximum Bandwidth: 0 (KBytes/s)
  - Traffic Priority: High
- Anti-Virus & Web filter:** ☐
  - Content Profile: Strict
- Log Traffic:** ☐
- Comments:** maximum 63 chars

At the bottom of the window are 'OK' and 'Cancel' buttons.

## IPSec VPN concentrators

In a hub-and-spoke network, all VPN tunnels terminate at a single VPN peer known as a hub. The peers that connect to the hub are known as spokes. The hub functions as a concentrator on the network, managing the VPN connections between the spokes.

The advantage of a hub-and-spoke network is that the spokes are simpler to configure because they require fewer policy rules. Also, a hub-and-spoke network provides some processing efficiencies, particularly on the spokes. The disadvantage of a hub-and-spoke network is its reliance on a single peer to handle management of all VPNs. If this peer goes down, all encrypted communication in the network is impossible.

A hub-and-spoke VPN network requires a special configuration. Setup varies depending on the role that the VPN peer is serving. If the VPN peer is a FortiGate unit functioning as the hub, or concentrator, it requires a VPN configuration connecting it to each spoke (AutoIKE phase 1 and 2 settings or manual key settings, plus encrypt policies). It also requires a concentrator configuration that groups the hub-and-spoke tunnels together. The concentrator configuration defines the FortiGate unit as the hub in a hub-and-spoke network.

If the VPN peer is one of the spokes, it requires a tunnel connecting it to the hub (but not to the other spokes). It also requires policies that control its encrypted connections to the other spokes and its non-encrypted connections to other networks, such as the Internet.

- [VPN concentrator \(hub\) general configuration steps](#)
- [Adding a VPN concentrator](#)
- [VPN spoke general configuration steps](#)

### VPN concentrator (hub) general configuration steps

A central FortiGate that is functioning as a hub requires the following configuration:

- A tunnel (AutoIKE phase 1 and phase 2 configuration or manual key configuration) for each spoke.
- Destination addresses for each spoke.
- A concentrator configuration.
- An encrypt policy for each spoke.

To create a VPN concentrator configuration:

- 1 Configure a tunnel for each spoke. Choose between a manual key tunnel or an AutoIKE tunnel.
  - A manual key tunnel consists of a name for the tunnel, the IP address of the spoke (client or gateway) at the opposite end of the tunnel, and the encryption and authentication algorithms to use for the tunnel.  
See [“Manual key IPSec VPNs” on page 183](#).
  - An AutoIKE tunnel consists of phase 1 and phase 2 parameters. The phase 1 parameters include the name of the spoke (client or gateway), designation of how the spoke receives its IP address (static or dialup), encryption and authentication algorithms, and the authentication method—either pre-shared keys or PKI certificates. The phase 2 parameters include the name of the tunnel, selection of the spoke (client or gateway) configured in phase 1, encryption and authentication algorithms, and a number of security parameters.  
See [“AutoIKE IPSec VPNs” on page 185](#).
- 2 Add a destination addresses for each spoke. The destination address is the address of the spoke (either a client on the Internet or a network located behind a gateway).  
See [“Adding a source address” on page 197](#).
- 3 Add the concentrator configuration. This step groups the tunnels together on the FortiGate unit. The tunnels link the hub to the spokes. The tunnels are added as part of the AutoIKE phase 2 configuration or the manual key configuration.  
See [“Adding a VPN concentrator” on page 201](#).



**Note:** Add the concentrator configuration to the central FortiGate unit (the hub) after adding the tunnels for all spokes.

- 4 Add an encrypt policy for each spoke. Encrypt policies control the direction of traffic through the hub and allow inbound and outbound VPN connections between the hub and the spokes. The encrypt policy for each spoke must include the tunnel name of the spoke. The source address must be Internal\_All. Use the following configuration for the encrypt policies:

|                       |                                  |
|-----------------------|----------------------------------|
| <b>Source</b>         | Internal_All                     |
| <b>Destination</b>    | The VPN spoke address.           |
| <b>Action</b>         | ENCRYPT                          |
| <b>VPN Tunnel</b>     | The VPN spoke tunnel name.       |
| <b>Allow inbound</b>  | Select allow inbound.            |
| <b>Allow outbound</b> | Select allow outbound            |
| <b>Inbound NAT</b>    | Select inbound NAT if required.  |
| <b>Outbound NAT</b>   | Select outbound NAT if required. |

See [“Adding an encrypt policy” on page 197](#).

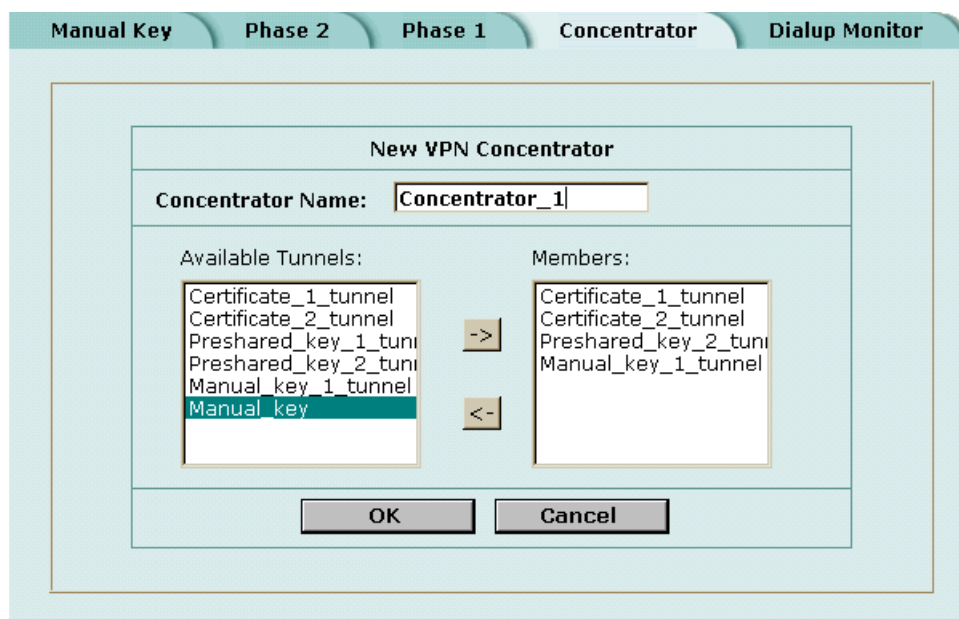
- 5 Arrange the policies in the following order:
  - encrypt policies
  - default non-encrypt policy (Internal\_All -> External\_All)

## Adding a VPN concentrator

To add a VPN concentrator configuration:

- 1 Go to **VPN > IPSec > Concentrator**.
- 2 Select New to add a VPN concentrator.
- 3 Enter the name of the new concentrator in the Concentrator Name field.
- 4 To add tunnels to the VPN concentrator, select a VPN tunnel from the Available Tunnels list and select the right arrow.
- 5 To remove tunnels from the VPN concentrator, select the tunnel in the Members list and select the left arrow.
- 6 Select OK to add the VPN concentrator.

Figure 26: Adding a VPN concentrator



## VPN spoke general configuration steps

A remote VPN peer that is functioning as a spoke requires the following configuration:

- A tunnel (AutoIKE phase 1 and phase 2 configuration or manual key configuration) for the hub.
- The source address of the local VPN spoke.
- The destination address of each remote VPN spoke.
- A separate outbound encrypt policy for each remote VPN spoke. These policies allow the local VPN spoke to initiate encrypted connections.
- A single inbound encrypt policy. This policy allows the local VPN spoke to accept encrypted connections.

To create a VPN spoke configuration:

- 1 Configure a tunnel between the spoke and the hub.  
Choose between a manual key tunnel or an AutoIKE tunnel.
  - To add a manual key tunnel, see [“Manual key IPSec VPNs” on page 183](#).
  - To add an AutoIKE tunnel, see: [“AutoIKE IPSec VPNs” on page 185](#).
- 2 Add the source address. One source address is required for the local VPN spoke.  
See [“Adding a source address” on page 197](#).
- 3 Add a destination addresses for each remote VPN spoke. The destination address is the address of the spoke (either a client on the Internet or a network located behind a gateway).  
See [“Adding a destination address” on page 197](#)
- 4 Add a separate outbound encrypt policy for each remote VPN spoke. These policies control the encrypted connections initiated by the local VPN spoke.  
The encrypt policy must include the appropriate source and destination addresses and the tunnel added in step 1. Use the following configuration:

|                       |                                                                                      |
|-----------------------|--------------------------------------------------------------------------------------|
| <b>Source</b>         | The local VPN spoke address.                                                         |
| <b>Destination</b>    | The remote VPN spoke address.                                                        |
| <b>Action</b>         | ENCRYPT                                                                              |
| <b>VPN Tunnel</b>     | The VPN tunnel name added in step 1. (Use the same tunnel for all encrypt policies.) |
| <b>Allow inbound</b>  | Do not enable.                                                                       |
| <b>Allow outbound</b> | Select allow outbound                                                                |
| <b>Inbound NAT</b>    | Select inbound NAT if required.                                                      |
| <b>Outbound NAT</b>   | Select outbound NAT if required.                                                     |

See [“Adding an encrypt policy” on page 197](#).

- 5 Add an inbound encrypt policy. This policies controls the encrypted connections initiated by the remote VPN spokes.  
The encrypt policy for the hub must include the appropriate source and destination addresses and the tunnel added in step 1. Use the following configuration:

|                    |                              |
|--------------------|------------------------------|
| <b>Source</b>      | The local VPN spoke address. |
| <b>Destination</b> | External_All                 |

|                                                              |                                                                                      |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------|
| <b>Action</b>                                                | ENCRYPT                                                                              |
| <b>VPN Tunnel</b>                                            | The VPN tunnel name added in step 1. (Use the same tunnel for all encrypt policies.) |
| <b>Allow inbound</b>                                         | Select allow inbound.                                                                |
| <b>Allow outbound</b>                                        | Do not enable.                                                                       |
| <b>Inbound NAT</b>                                           | Select inbound NAT if required.                                                      |
| <b>Outbound NAT</b>                                          | Select outbound NAT if required.                                                     |
| See <a href="#">“Adding an encrypt policy” on page 197</a> . |                                                                                      |

- 6 Arrange the policies in the following order:
- outbound encrypt policies
  - inbound encrypt policy
  - default non-encrypt policy (Internal\_All -> External\_All)



**Note:** The default non-encrypt policy is required to allow the VPN spoke to access other networks, such as the Internet.

## Redundant IPSec VPNs

To ensure the continuous availability of an IPSec VPN tunnel, you can configure multiple connections between the local the FortiGate unit and the remote VPN peer (remote gateway). With a redundant configuration, if one connection fails the FortiGate unit will establish a tunnel using the other connection.

Configuration depends on the number of connections that each VPN peer has to the Internet. For example, if the local VPN peer has two connections to the Internet, then it can provide two redundant connections to the remote VPN peer.

A single VPN peer can be configured with up to three redundant connections.

The VPN peers are not required to have a matching number of Internet connections. For example, between two VPN peers, one can have multiple Internet connections while the other has only one Internet connection. Of course, with an asymmetrical configuration, the level redundancy will vary from one end of the VPN to the other.



**Note:** IPSec Redundancy is only available to VPN peers that have static IP addresses and that authenticate themselves to each other with pre-shared keys or digital certificates. It is not available to VPN peers that have dynamically assigned IP addresses (dialup users). Nor is it available to VPN peers that use manual keys.

### Configuring redundant IPSec VPN

Prior to configuring the VPN, make sure that both FortiGate units have multiple connections to the Internet. For each unit, first add multiple (two or more) external interfaces. Then assign each interface to an external zone. Finally, add a route to the Internet through each interface.

Configure the two FortiGate units with symmetrical settings for their connections to the Internet. For example, if the remote FortiGate unit has two external interfaces grouped within one zone, then the local FortiGate unit should have two external interfaces grouped within one zone.

Similarly, if the remote FortiGate has two external interfaces in separate zones, then the local FortiGate unit should have two external interfaces in separate zones.

Configuration is made simpler if all external interfaces are grouped within a single zone, rather than multiple zones. However, this may not always be possible due to security considerations or other reasons.

After you have defined the Internet connections for both FortiGate units, you can proceed to configure the VPN tunnel.

To configure IPSec redundancy:

- 1 Add the phase 1 parameters for up to three VPN connections.  
Enter identical values for each VPN connection, with the exception of the Gateway Name and IP Address. Make sure that the remote VPN peer (Remote Gateway) has a static IP address.  
See [“Adding a phase 1 configuration for an AutoIKE VPN” on page 185](#).
- 2 Add the phase 2 parameters (VPN tunnel) for up to three VPN connections.
  - If the Internet connections are in the same zone, add one VPN tunnel and add the remote gateways to it. You can add up to three remote gateways.
  - If the Internet connections are in separate zones or assigned to unique interfaces, add a VPN tunnel for each remote gateway entered.  
See [“Adding a phase 2 configuration for an AutoIKE VPN” on page 189](#).
- 3 Add the source and destination addresses.  
See [“Adding a source address” on page 197](#).  
See [“Adding a destination address” on page 197](#).
- 4 Add encrypt policies for up to three VPN connections.
  - If the VPN connections are in the same zone, add one outgoing encrypt policy; for example an Internal->External policy. Add the AutoIKE key tunnel to this policy.
  - If the VPN connections are in different zones, add a separate outgoing encrypt policy for each connection; for example, an Internal->External and an Internal->DMZ policy. The source and destination of both policies must be the same. Add a different AutoIKE key tunnel to each policy.  
See [“Adding an encrypt policy” on page 197](#).

## Monitoring and Troubleshooting VPNs

This section provides a number of general maintenance and monitoring procedures for VPNs.

This section describes:

- [Viewing VPN tunnel status](#)
- [Viewing dialup VPN connection status](#)
- [Testing a VPN](#)

### Viewing VPN tunnel status

You can use the IPSec VPN tunnel list to view the status of all IPSec AutoIKE key VPN tunnels. For each tunnel, the list shows the status of each tunnel as well as the tunnel time out.

To view VPN tunnel status:

- 1 Go to **VPN > IPSEC > AutoIKE Key**.

The Status column displays the status of each tunnel. If Status is Up, the tunnel is active. If Status is Down, the tunnel is not active.

The Timeout column displays the time before the next key exchange. The time is calculated by subtracting the time elapsed since the last key exchange from the keylife.

**Figure 27: AutoIKE key tunnel status**

| Manual Key   Phase 2   Phase 1   Concentrator   Dialup Monitor |                |                  |        |         |                                                                                                                                                                             |
|----------------------------------------------------------------|----------------|------------------|--------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tunnel Name                                                    | Remote Gateway | Lifetime(sec/kb) | Status | Timeout | Modify                                                                                                                                                                      |
| AutoIKE_tunnel_1                                               | 66.34.23.78    | 300/10240        | Up     | 87      |   |
| AutoIKE_tunnel_2                                               | 55.66.77.88    | 300/NA           | Down   | 0       |                                                                                        |
| <div>New</div>                                                 |                |                  |        |         |                                                                                                                                                                             |

### Viewing dialup VPN connection status

You can use the dialup monitor to view the status of dialup VPNs. The dialup monitor lists the remote gateways and the active VPN tunnels for each gateway. The monitor also lists the tunnel lifetime, timeout, proxy ID source, and proxy ID destination for each tunnel.

To view dialup connection status:

**1 Go to VPN > IPSec > Dialup.**

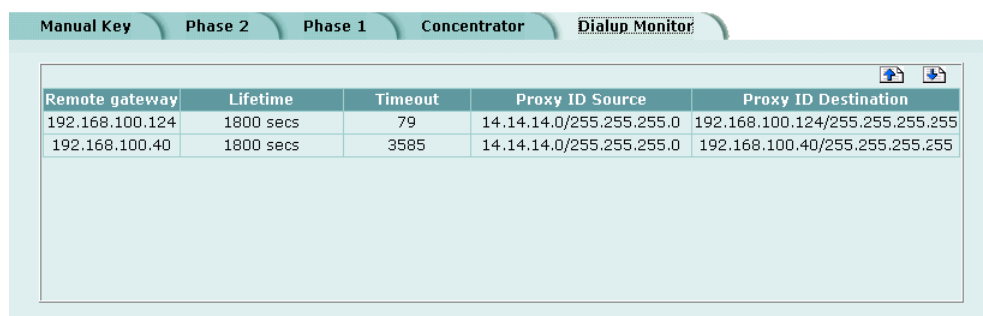
The Lifetime column displays how long the connection has been up.

The Timeout column displays the time before the next key exchange. The time is calculated by subtracting the time elapsed since the last key exchange from the keylife.

The Proxy ID Source column displays the actual IP address or subnet address of the remote peer.

The Proxy ID Destination column displays the actual IP address or subnet address of the local peer.

**Figure 28: Dialup Monitor**



| Remote gateway  | Lifetime  | Timeout | Proxy ID Source          | Proxy ID Destination            |
|-----------------|-----------|---------|--------------------------|---------------------------------|
| 192.168.100.124 | 1800 secs | 79      | 14.14.14.0/255.255.255.0 | 192.168.100.124/255.255.255.255 |
| 192.168.100.40  | 1800 secs | 3585    | 14.14.14.0/255.255.255.0 | 192.168.100.40/255.255.255.255  |

## Testing a VPN

To confirm that a VPN between two networks has been configured correctly, use the ping command from one internal network to connect to a computer on the other internal network. The IPSec VPN tunnel starts automatically when the first data packet destined for the VPN is intercepted by the FortiGate unit.

To confirm that a VPN between a network and one or more clients has been configured correctly, start a VPN client and use the ping command to connect to a computer on the internal network. The VPN tunnel initializes automatically when the client makes a connection attempt. You can start the tunnel and test it at the same time by pinging from the client to an address on the internal network.

# PPTP and L2TP VPN

You can use PPTP and L2TP to create a virtual private network (VPN) between a remote client PC running the Windows operating system and your internal network. Because they are Windows standards, PPTP and L2TP do not require third-party software on the client computer. So long as the Internet Service Provider supports PPTP and L2TP connections, you can create a secure connection by making relatively simple configuration changes to the client computer and the FortiGate unit.

This chapter provides an overview of how to configure FortiGate PPTP and L2TP VPN. For a complete description of FortiGate PPTP and L2TP, see the *FortiGate VPN Guide*.

This chapter describes:

- [Configuring PPTP](#)
- [Configuring L2TP](#)

## Configuring PPTP

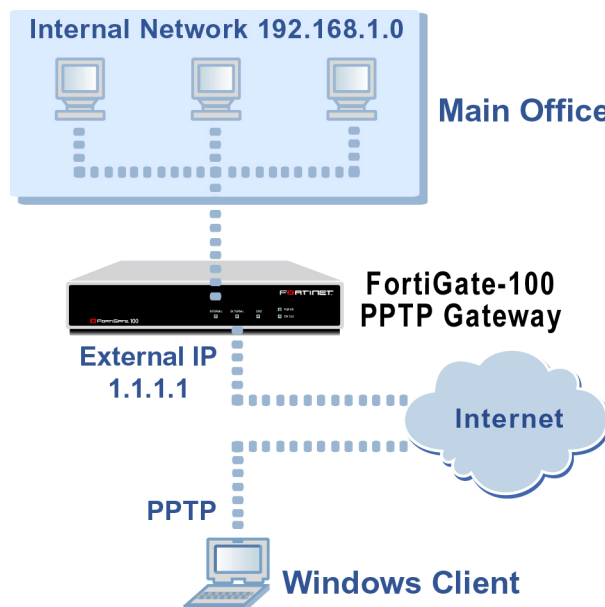
As its name suggests, PPTP involves the Point-to-Point protocol. PPTP packages data within PPP packets and then encapsulates the PPP packets within IP packets for transmission through a VPN tunnel.



**Note:** PPTP VPNs are only supported in NAT/Route mode.

This section describes:

- [Configuring the FortiGate unit as a PPTP gateway](#)
- [Configuring a Windows 98 client for PPTP](#)
- [Configuring a Windows 2000 client for PPTP](#)
- [Configuring a Windows XP client for PPTP](#)

**Figure 29: PPTP VPN between a Windows client and the FortiGate unit**

## Configuring the FortiGate unit as a PPTP gateway

Use the following procedures to configure the FortiGate unit as a PPTP gateway:

### Adding users and user groups

To add a user for each PPTP client:

- 1 Go to **User > Local**.
- 2 Add and configure PPTP users.  
See [“Adding user names and configuring authentication” on page 174](#).
- 3 Go to **User > User Group**.
- 4 Add and configure PPTP user groups.  
See [“Configuring user groups” on page 179](#).

### Enabling PPTP and specifying an address range

- 1 Go to **VPN > PPTP > PPTP Range**.
- 2 Select **Enable PPTP**.
- 3 Enter the Starting IP and the Ending IP for the PPTP address range.
- 4 Select the User Group that you added in [“Adding users and user groups” on page 208](#).
- 5 Select **Apply** to enable PPTP through the FortiGate unit.

**Figure 30: Example PPTP Range configuration**

### Adding a source address

Add a source address for every address in the PPTP address range.

- 1 Go to **Firewall > Address**.
- 2 Select the interface to which PPTP clients connect.
- 3 Select New to add an address.
- 4 Enter the Address Name, IP Address, and NetMask for an address in the PPTP address range.
- 5 Select OK to save the source address.
- 6 Repeat for all addresses in the PPTP address range.



**Note:** If the PPTP address range is comprised of an entire subnet, add an address for this subnet. Do not add an address group.

### Adding an address group

Organize the source addresses into an address group.

- 1 Go to **Firewall > Address > Group**.
- 2 Add a new address group to the interface to which PPTP clients connect.
- 3 Enter a Group Name to identify the address group.  
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.
- 4 To add addresses to the address group, select an address from the Available Addresses list and select the right arrow to add it to the Members list.
- 5 To remove addresses from the address group, select an address from the Members list and select the left arrow to remove it from the group.  
Select OK to add the address group.

### Adding a destination address

Add an address to which PPTP users can connect.

- 1 Go to **Firewall > Address**.
- 2 Select the internal interface or the DMZ interface. (Methods will differ slightly between FortiGate models.)
- 3 Select New to add an address.
- 4 Enter the Address Name, IP Address, and NetMask for a single computer or for an entire subnet on an internal interface of the local VPN peer.
- 5 Select OK to save the source address.

### Adding a firewall policy

Add a policy which specifies the source and destination addresses and sets the service for the policy to the traffic type inside the PPTP VPN tunnel.

- 1 Go to **Firewall > Policy**.
- 2 Select the policy list to which you want to add the policy.
- 3 Select New to add a new policy.
- 4 Set Source to the group that matches the PPTP address range.
- 5 Set Destination to the address to which PPTP users can connect.
- 6 Set Service to match the traffic type inside the PPTP VPN tunnel.  
For example, if PPTP users can access a web server, select HTTP.
- 7 Set Action to ACCEPT.
- 8 Select NAT if address translation is required.  
You can also configure traffic shaping, logging, and antivirus and web filter settings for PPTP policies.
- 9 Select OK to save the firewall policy.

## Configuring a Windows 98 client for PPTP

Use the following procedure to configure a client computer running Windows 98 so that it can connect to a FortiGate PPTP VPN. To configure the Windows 98 client, you must install and configure Windows dialup networking and virtual private networking support.

### Installing PPTP support

- 1 Go to **Start > Settings > Control Panel > Network**.
- 2 Select Add.
- 3 Select Adapter.
- 4 Select Add.
- 5 Select Microsoft as the manufacturer.
- 6 Select Microsoft Virtual Private Networking Adapter.
- 7 Select OK twice.

- 8 Insert diskettes or CDs as required.
- 9 Restart the computer.

### **Configuring a PPTP dialup connection**

- 1 Go to **My Computer > Dial-Up Networking > Configuration**.
- 2 Double-click Make New Connection.
- 3 Name the connection and select Next.
- 4 Enter the IP address or host name of the FortiGate unit to connect to and select Next.
- 5 Select Finish.  
An icon for the new connection appears in the Dial-Up Networking folder.
- 6 Right-click the new icon and select Properties.
- 7 Go to Server Types.
- 8 Uncheck IPX/SPX Compatible.
- 9 Select TCP/IP Settings.
- 10 Uncheck Use IP header compression.
- 11 Uncheck Use default gateway on remote network.
- 12 Select OK twice.

### **Connecting to the PPTP VPN**

- 1 Start the dialup connection that you configured in the previous procedure.
- 2 Enter your PPTP VPN User Name and Password.
- 3 Select Connect.

## **Configuring a Windows 2000 client for PPTP**

Use the following procedure to configure a client computer running Windows 2000 so that it can connect to a FortiGate PPTP VPN.

### **Configuring a PPTP dialup connection**

- 1 Go to **Start > Settings > Network and Dial-up Connections**.
- 2 Double-click Make New Connection to start the Network Connection Wizard and select Next.
- 3 For Network Connection Type, select Connect to a private network through the Internet and select Next.
- 4 For Destination Address, enter the IP address or host name of the FortiGate unit to connect to and select Next.
- 5 Set Connection Availability to Only for myself and select Next.
- 6 Select Finish.
- 7 In the Connect window, select Properties.
- 8 Select the Security tab.

- 9 Uncheck Require data encryption.
- 10 Select OK.

### Connecting to the PPTP VPN

- 1 Start the dialup connection that you configured in the previous procedure.
- 2 Enter your PPTP VPN User Name and Password.
- 3 Select Connect.
- 4 In the connect window, enter the User Name and Password that you use to connect to your dialup network connection.  
This user name and password is not the same as your VPN user name and password.

## Configuring a Windows XP client for PPTP

Use the following procedure to configure a client computer running Windows XP so that it can connect to a FortiGate PPTP VPN.

### Configuring a PPTP dialup connection

- 1 Go to **Start > Control Panel**.
- 2 Select Network and Internet Connections.
- 3 Select Create a Connection to the network of your workplace and select Next.
- 4 Select Virtual Private Network Connection and select Next.
- 5 Name the connection and select Next.
- 6 If the Public Network dialog box appears, choose the appropriate initial connection and select Next.
- 7 In the VPN Server Selection dialog, enter the IP address or host name of the FortiGate unit to connect to and select Next.
- 8 Select Finish.

### Configuring the VPN connection

- 1 Right-click the Connection icon that you created in the previous procedure.
- 2 Select **Properties > Security**.
- 3 Select Typical to configure typical settings.
- 4 Select Require data encryption.



**Note:** If a RADIUS server is used for authentication do not select Require data encryption. PPTP encryption is not supported for RADIUS server authentication.

- 5 Select Advanced to configure advanced settings.
- 6 Select Settings.
- 7 Select Challenge Handshake Authentication Protocol (CHAP).
- 8 Make sure that none of the other settings are selected.

- 9 Select the Networking tab.
- 10 Make sure that the following options are selected:
  - TCP/IP
  - QoS Packet Scheduler
- 11 Make sure that the following options are not selected:
  - File and Printer Sharing for Microsoft Networks
  - Client for Microsoft Networks
- 12 Select OK.

### Connecting to the PPTP VPN

- 1 Connect to your ISP.
- 2 Start the VPN connection that you configured in the previous procedure.
- 3 Enter your PPTP VPN User Name and Password.
- 4 Select Connect.
- 5 In the connect window, enter the User Name and Password that you use to connect to your dialup network connection.

This user name and password is not the same as your VPN user name and password.

## Configuring L2TP

Some implementations of L2TP support elements of IPSec. These elements must be disabled when L2TP is used with Fortigate units.

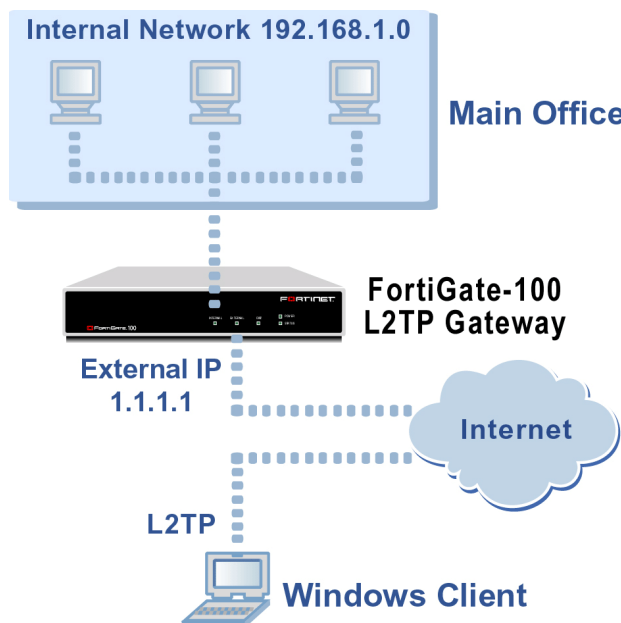


**Note:** L2TP VPNs are only supported in NAT/Route mode.

This section describes:

- [Configuring the FortiGate unit as a L2TP gateway](#)
- [Configuring a Windows 2000 client for L2TP](#)
- [Configuring a Windows XP client for L2TP](#)

Figure 31: L2TP VPN between a Windows client and the FortiGate unit



## Configuring the FortiGate unit as a L2TP gateway

Use the following procedures to configure the FortiGate unit as an L2TP gateway:

### Adding users and user groups

To add a user for each L2TP client:

- 1 Go to **User > Local**.
- 2 Add and configure L2TP users.  
See [“Adding user names and configuring authentication” on page 174](#).
- 3 Go to **User > User Group**.
- 4 Add and configure L2TP user groups.  
See [“Configuring user groups” on page 179](#).

### Enabling L2TP and specifying an address range

- 1 Go to **VPN > L2TP > L2TP Range**.
- 2 Select **Enable L2TP**.
- 3 Enter the Starting IP and the Ending IP for the L2TP address range.
- 4 Select the User Group that you added in [“Adding users and user groups” on page 214](#).
- 5 Select **Apply** to enable L2TP through the FortiGate unit.

**Figure 32: Sample L2TP address range configuration**

- 6 Add the addresses from the L2TP address range to the external interface address list. The addresses can be grouped into an external address group.
- 7 Add addresses to the destination interface address list to control the addresses to which L2TP clients can connect. The addresses can be grouped into an address group.  
For example, if you want L2TP users to connect to the internal network, go to Firewall > Address > Internal and add addresses to the internal interface address list.
- 8 Add a policy to allow L2TP clients to connect through the FortiGate unit.

### Adding a source address

Add a source address for every address in the L2TP address range.

- 1 Go to **Firewall > Address**.
- 2 Select the interface to which L2TP clients connect.
- 3 Select New to add an address.
- 4 Enter the Address Name, IP Address, and NetMask for an address in the L2TP address range.
- 5 Select OK to save the source address.
- 6 Repeat for all addresses in the L2TP address range.



**Note:** If the L2TP address range is comprised of an entire subnet, add an address for this subnet. Do not add an address group.

### Adding an address group

Organize the source addresses into an address group.

- 1 Go to **Firewall > Address > Group**.
- 2 Add a new address group to the interface to which L2TP clients connect.

- 3 Enter a Group Name to identify the address group.  
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Other special characters and spaces are not allowed.
- 4 To add addresses to the address group, select an address from the Available Addresses list and select the right arrow to add it to the Members list.
- 5 To remove addresses from the address group, select an address from the Members list and select the left arrow to remove it from the group.  
Select OK to add the address group.

### **Adding a destination address**

Add an address to which L2TP users can connect.

- 1 Go to **Firewall > Address**.
- 2 Select the internal interface or the DMZ interface. (Methods will differ slightly between FortiGate models.)
- 3 Select New to add an address.
- 4 Enter the Address Name, IP Address, and NetMask for a single computer or for an entire subnetwork on an internal interface of the local VPN peer.
- 5 Select OK to save the source address.

### **Adding a firewall policy**

Add a policy which specifies the source and destination addresses and sets the service for the policy to the traffic type inside the L2TP VPN tunnel.

- 1 Go to **Firewall > Policy**.
- 2 Select the policy list to which you want to add the policy.
- 3 Select New to add a new policy.
- 4 Set Source to the group that matches the L2TP address range.
- 5 Set Destination to the address to which L2TP users can connect.
- 6 Set Service to match the traffic type inside the L2TP VPN tunnel.  
For example, if L2TP users can access a web server, select HTTP.
- 7 Set Action to ACCEPT.
- 8 Select NAT if address translation is required.  
You can also configure traffic shaping, logging, and antivirus and web filter settings for L2TP policies.
- 9 Select OK to save the firewall policy.

## Configuring a Windows 2000 client for L2TP

Use the following procedure to configure a client computer running Windows 2000 so that it can connect to a FortiGate L2TP VPN.

### Configuring an L2TP dialup connection

- 1 Go to **Start > Settings > Network and Dial-up Connections**.
- 2 Double-click Make New Connection to start the Network Connection Wizard and select Next.
- 3 For Network Connection Type, select Connect to a private network through the Internet and select Next.
- 4 For Destination Address, enter the address of the FortiGate unit to connect to and select Next.
- 5 Set Connection Availability to Only for myself and select Next.
- 6 Select Finish.
- 7 In the Connect window, select Properties.
- 8 Select the Security tab.
- 9 Make sure that Require data encryption is selected.



**Note:** If a RADIUS server is used for authentication do not select Require data encryption. L2TP encryption is not supported for RADIUS server authentication.

- 10 Select the Networking tab.
- 11 Set VPN server type to Layer-2 Tunneling Protocol (L2TP).
- 12 Save your changes and continue with the following procedure.

### Disabling IPSec

- 1 Select the Networking tab.
- 2 Select Internet Protocol (TCP/IP) properties.
- 3 Double-click the Advanced tab.
- 4 Go to the Options tab and select IP security properties.
- 5 Make sure that Do not use IPSEC is selected.
- 6 Select OK and close the connection properties window.



**Note:** The default Windows 2000 L2TP traffic policy does not allow L2TP traffic without IPSec encryption. You can disable default behavior by editing the Windows 2000 Registry as described in the following steps. See the Microsoft documentation for editing the Windows Registry.

- 7 Use the registry editor (regedit) to locate the following key in the registry:  
HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters

- 8 Add the following registry value to this key:  
Value Name: ProhibitIpSec  
Data Type: REG\_DWORD  
Value: 1
- 9 Save your changes and restart the computer for the changes to take effect.  
You must add the ProhibitIpSec registry value to each Windows 2000-based endpoint computer of an L2TP or IPSec connection to prevent the automatic filter for L2TP and IPSec traffic from being created. When the ProhibitIpSec registry value is set to 1, your Windows 2000-based computer does not create the automatic filter that uses CA authentication. Instead, it checks for a local or active directory IPSec policy.

### Connecting to the L2TP VPN

- 1 Start the dialup connection that you configured in the previous procedure.
- 2 Enter your L2TP VPN User Name and Password.
- 3 Select Connect.
- 4 In the connect window, enter the User Name and Password that you use to connect to your dialup network connection.  
This user name and password is not the same as your VPN user name and password.

## Configuring a Windows XP client for L2TP

Use the following procedure to configure a client computer running Windows XP so that it can connect to a FortiGate L2TP VPN.

### Configuring an L2TP VPN dialup connection

- 1 Go to **Start > Settings**.
- 2 Select Network and Internet Connections.
- 3 Select Create a connection to the network of your workplace and select Next.
- 4 Select Virtual Private Network Connection and select Next.
- 5 Name the connection and select Next.
- 6 If the Public Network dialog box appears, choose the appropriate initial connection and select Next.
- 7 In the VPN Server Selection dialog, enter the IP address or host name of the FortiGate unit to connect to and select Next.
- 8 Select Finish.

### Configuring the VPN connection

- 1 Right-click the icon that you have created.
- 2 Select **Properties > Security**.
- 3 Select Typical to configure typical settings.
- 4 Select Require data encryption.



**Note:** If a RADIUS server is used for authentication do not select Require data encryption. L2TP encryption is not supported for RADIUS server authentication.

- 5 Select Advanced to configure advanced settings.
- 6 Select Settings.
- 7 Select Challenge Handshake Authentication Protocol (CHAP).
- 8 Make sure that none of the other settings are selected.
- 9 Select the Networking tab.
- 10 Make sure that the following options are selected:
  - TCP/IP
  - QoS Packet Scheduler
- 11 Make sure that the following options are not selected:
  - File and Printer Sharing for Microsoft Networks
  - Client for Microsoft Networks

### Disabling IPsec

- 1 Select the Networking tab.
- 2 Select Internet Protocol (TCP/IP) properties.
- 3 Double-click the Advanced tab.
- 4 Go to the Options tab and select IP security properties.
- 5 Make sure that Do not use IPSEC is selected.
- 6 Select OK and close the connection properties window.



**Note:** The default Windows XP L2TP traffic policy does not allow L2TP traffic without IPsec encryption. You can disable default behavior by editing the Windows XP Registry as described in the following steps. See the Microsoft documentation for editing the Windows Registry.

- 7 Use the registry editor (regedit) to locate the following key in the registry:  
HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
- 8 Add the following registry value to this key:  
Value Name: ProhibitIpSec  
Data Type: REG\_DWORD  
Value: 1
- 9 Save your changes and restart the computer for the changes to take effect.

You must add the ProhibitIpSec registry value to each Windows XP-based endpoint computer of an L2TP or IPsec connection to prevent the automatic filter for L2TP and IPsec traffic from being created. When the ProhibitIpSec registry value is set to 1, your Windows XP-based computer does not create the automatic filter that uses CA authentication. Instead, it checks for a local or active directory IPsec policy.

**Connecting to the L2TP VPN**

- 1** Connect to your ISP.
- 2** Start the VPN connection that you configured in the previous procedure.
- 3** Enter your L2TP VPN User Name and Password.
- 4** Select Connect.
- 5** In the connect window, enter the User Name and Password that you use to connect to your dialup network connection.  
This user name and password is not the same as your VPN user name and password.

# Network Intrusion Detection System (NIDS)

The FortiGate NIDS is a real-time network intrusion detection sensor that uses attack signature definitions to both detect and prevent a wide variety of suspicious network traffic and direct network-based attacks. Also, whenever an attack occurs, the FortiGate NIDS can record the event in a log plus send an alert email to the system administrator.

This chapter describes:

- [Detecting attacks](#)
- [Preventing attacks](#)
- [Logging attacks](#)

## Detecting attacks

The NIDS Detection module detects a wide variety of suspicious network traffic and network-based attacks. Use the following procedures to configure the general NIDS settings and the NIDS Detection module Signature List.

For the general NIDS settings, you need to select which interfaces will be monitored for network-based attacks. You also need to decide whether to enable checksum verification. Checksum verification tests the integrity of packets received at the monitored interface(s).

This section describes:

- [Selecting the interfaces to monitor](#)
- [Disabling the NIDS](#)
- [Configuring checksum verification](#)
- [Viewing the signature list](#)
- [Viewing attack descriptions](#)
- [Enabling and disabling NIDS attack signatures](#)
- [Adding user-defined signatures](#)

### Selecting the interfaces to monitor

- 1 Go to **NIDS > Detection > General**.
- 2 Select the interfaces to monitor for network attacks.  
You can select one or more interfaces.
- 3 Select Apply.

### Disabling the NIDS

- 1 Go to **NIDS > Detection > General**.
- 2 Deselect all monitored interfaces.
- 3 Select Apply.

### Configuring checksum verification

Checksum verification tests files passing through the FortiGate unit to make sure that they have not been changed in transit. The NIDS can run checksum verification on IP, TCP, UDP, and ICMP traffic. For maximum detection, you can turn on checksum verification for all types of traffic. However, if the FortiGate unit does not need to run checksum verification, you can turn it off for some or all types of traffic to improve system performance. For example, you might not need to run checksum verification if your FortiGate unit is installed behind a router that also does checksum verification.

- 1 Go to **NIDS > Detection > General**.
- 2 Check the type of traffic on which to run Checksum Verifications.
- 3 Select Apply.

Figure 33: Example NIDS detection configuration

The screenshot shows the 'General' tab of the NIDS detection configuration. The 'Monitored Interface' section has four radio buttons: 'none', 'internal', 'external' (selected), and 'dmz'. The 'Checksum Verifications' section has four checkboxes: 'IP' (checked), 'TCP' (unchecked), 'UDP' (unchecked), and 'ICMP' (unchecked). An 'Apply' button is located at the bottom of the configuration area.

## Viewing the signature list

To display the current list of NIDS signature groups and to view the members of a signature group:

- 1 Go to **NIDS > Detection > Signature List**.
- 2 View the names and action status of the signature groups in the list.  
The NIDS detects attacks listed in all the signature groups that are checked in the Modify or Details column.



**Note:** The user-defined signature group is the last item in the signature list. See [“Adding user-defined signatures” on page 224](#).

- 3 Select View Details to display the members of a signature group.  
The Signature Group Members list displays the attack ID, Rule Name, and Revision number for each group member.

## Viewing attack descriptions

Fortinet provides online information for all NIDS attacks. To view the FortiResponse Attack Analysis web page for an attack listed on the signature list:

- 1 Go to **NIDS > Detection > Signature List**.
- 2 Select View Details to display the members of a signature group.  
Select a signature and copy its attack ID.
- 3 Open a web browser and enter this URL:  
`http://www.fortinet.com/ids/ID<attack-ID>`  
Remember to include the attack ID.

For example, to view the Fortinet Attack Analysis web page for the ssh CRC32 overflow /bin/sh attack (ID 101646338), use the following URL:

<http://www.fortinet.com/ids/ID101646338>



**Note:** Each attack log message includes a URL that links directly to the FortiResponse Attack Analysis web page for that attack. This URL is available from the Attack Log messages and Alert email messages. For information about log message content and formats, and about log locations, see the *Logging Configuration and Reference Guide*. To log attack messages, see [“Logging attacks” on page 228](#).

**Figure 34: Example signature group members list**

| exploit   |                                   |          |
|-----------|-----------------------------------|----------|
| ID        | Rule Name                         | Revision |
| 101646337 | gobbles SSH exploit attempt       | 16       |
| 101646338 | ssh CRC32 overflow /bin/sh        | 16       |
| 101646339 | ssh CRC32 overflow NOOP           | 16       |
| 101646340 | ssh CRC32 overflow                | 16       |
| 101646341 | x86 linux samba overflow          | 16       |
| 101646342 | Solaris x86 nlps overflow attempt | 16       |
| 101646343 | nlps x86 solaris overflow         | 16       |
| 101646344 | LPRng overflow                    | 16       |
| 101646345 | redhat 7.0 lprd overflow          | 16       |

## Enabling and disabling NIDS attack signatures

By default, all NIDS attack signatures are enabled. You can use the NIDS signature list to disable detection of some attacks. Disabling unnecessary NIDS attack signatures can improve system performance and reduce the number of IDS log messages and alert emails that the NIDS generates. For example, the NIDS detects a large number of web server attacks. If you do not provide access to a web server behind your firewall, you might want to disable all web server attack signatures.



**Note:** To save your NIDS attack signature settings, Fortinet recommends that you back up your FortiGate configuration before you update the firmware and restore the saved configuration after the update.

To disable NIDS attack signatures:

- 1 Go to **NIDS > Detection > Signature List**.
- 2 Scroll down the signature list to find the signature group to disable.  
Attack ID numbers and rule names in attack log messages and alert email match those in the signature group members list. You can scroll through a signature group members list to locate specific attack signatures by ID number and name.
- 3 Uncheck the Enable check box.
- 4 Select OK.
- 5 Repeat steps 2 to 4 for each NIDS attack signature group that you want to disable.  
Select Check All  to enable all NIDS attack signature groups in the signature list.  
Select Uncheck All  to disable all NIDS attack signature groups in the signature list.

## Adding user-defined signatures

You can create a user-defined signature list in a text file and upload it from the management computer to the FortiGate unit.

For information about how to write user-defined signatures, see the *FortiGate NIDS Guide*.

- 1 Go to **NIDS > Detection > User Defined Signature List**.
- 2 Select Upload.
- 3 Type the path and filename of the text file for the user-defined signature list or select Browse and locate the file.
- 4 Select OK to upload the text file for the user-defined signature list.
- 5 Select Return to display the uploaded user-defined signature list.

Figure 35: Example user-defined signature list

| User Defined Signature Detail |                       |          |
|-------------------------------|-----------------------|----------|
| ID                            | Rule Name             | Revision |
| 298319873                     | TFTP GET Admin.dll    | 1        |
| 113770498                     | Possible SYN FIN scan | 1        |
| 113770499                     | CGI-PHF access        | 1        |

### Downloading the user-defined signature list

You can back up the user-defined signature list by downloading it to a text file on the management computer.

- 1 Go to **NIDS > Detection > User Defined Signature List**.
- 2 Select Download.

The FortiGate unit downloads the user-defined signature list to a text file on the management computer. You can specify a location to which to download the text file as well as a name for the text file.

## Preventing attacks

NIDS attack prevention protects the FortiGate unit and the networks connected to it from common TCP, ICMP, UDP, and IP attacks. You can enable the NIDS attack prevention to prevent a set of default attacks with default threshold values. You can also enable and set the threshold values for individual attack signatures.



**Note:** After the FortiGate unit reboots, the NIDS attack prevention and synflood prevention are always disabled.

- [Enabling NIDS attack prevention](#)
- [Enabling NIDS attack prevention signatures](#)
- [Setting signature threshold values](#)
- [Configuring synflood signature values](#)

### Enabling NIDS attack prevention

- 1 Go to **NIDS > Prevention**.
- 2 Select Enable in the top left corner.

## Enabling NIDS attack prevention signatures

The NIDS Prevention module contains signatures that are designed to protect your network against attacks. Some signatures are enabled by default; others must be enabled. For a complete list of NIDS Prevention signatures and descriptions, see the *FortiGate NIDS Guide*.

- 1 Go to **NIDS > Prevention**.
- 2 Check the box in the Enable column beside each signature that you want to enable.
- 3 Select Check All  to enable all signatures in the NIDS attack prevention signature list.
- 4 Select Uncheck All  to disable all signatures in the NIDS attack prevention signature list.
- 5 Select Reset to Default Values  to enable only the default NIDS attack prevention signatures and return to the default threshold values.

Figure 36: Example NIDS attack prevention signature list entries

| Prevention                                                                                                                                                                                                                                                                                                        |                             |          |                                     |                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|----------|-------------------------------------|---------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> Enable Prevention    |                             |          |                                     |                                                                                       |
| Signature Abbreviation                                                                                                                                                                                                                                                                                            | Summary                     | Protocol | Enable                              | Modify                                                                                |
| synflood                                                                                                                                                                                                                                                                                                          | syn flood attack            | TCP      | <input checked="" type="checkbox"/> |   |
| portscan                                                                                                                                                                                                                                                                                                          | port scan attack            | TCP      | <input checked="" type="checkbox"/> |  |
| synfrag                                                                                                                                                                                                                                                                                                           | syn fragment attack         | TCP      | <input type="checkbox"/>            |                                                                                       |
| synfin                                                                                                                                                                                                                                                                                                            | syn with fin attack         | TCP      | <input type="checkbox"/>            |                                                                                       |
| noflag                                                                                                                                                                                                                                                                                                            | tcp with no flag attack     | TCP      | <input type="checkbox"/>            |                                                                                       |
| finnoack                                                                                                                                                                                                                                                                                                          | fin without ack attack      | TCP      | <input checked="" type="checkbox"/> |                                                                                       |
| srcsession                                                                                                                                                                                                                                                                                                        | source session limit        | TCP      | <input type="checkbox"/>            |  |
| winnuke                                                                                                                                                                                                                                                                                                           | winnuke attack              | TCP      | <input type="checkbox"/>            |                                                                                       |
| land                                                                                                                                                                                                                                                                                                              | tcp land attack             | TCP      | <input type="checkbox"/>            |                                                                                       |
| ftpvovfl                                                                                                                                                                                                                                                                                                          | ftp buffer overflow attack  | TCP      | <input type="checkbox"/>            |  |
| smtpvovfl                                                                                                                                                                                                                                                                                                         | smtp buffer overflow attack | TCP      | <input type="checkbox"/>            |  |
| pop3ovfl                                                                                                                                                                                                                                                                                                          | pop3 buffer overflow attack | TCP      | <input checked="" type="checkbox"/> |  |
| url                                                                                                                                                                                                                                                                                                               | invalid url attack          | TCP      | <input type="checkbox"/>            |                                                                                       |
| udpflood                                                                                                                                                                                                                                                                                                          | udp flood attack            | UDP      | <input type="checkbox"/>            |  |
| udpland                                                                                                                                                                                                                                                                                                           | udp land attack             | UDP      | <input type="checkbox"/>            |                                                                                       |
| udpsrcsession                                                                                                                                                                                                                                                                                                     | udp source session limit    | UDP      | <input type="checkbox"/>            |  |
| icmpflood                                                                                                                                                                                                                                                                                                         | icmp flood attack           | ICMP     | <input checked="" type="checkbox"/> |  |
| icmpfrag                                                                                                                                                                                                                                                                                                          | icmp fragment attack        | ICMP     | <input checked="" type="checkbox"/> |                                                                                       |
| icmpdeath                                                                                                                                                                                                                                                                                                         | ping of death attack        | ICMP     | <input type="checkbox"/>            |                                                                                       |
| icmplarge                                                                                                                                                                                                                                                                                                         | large icmp packet attack    | ICMP     | <input type="checkbox"/>            |  |

## Setting signature threshold values

You can change the default threshold values for the NIDS Prevention signatures listed in [Table 6](#). The threshold depends on the type of attack. For flooding attacks, the threshold is the maximum number of packets received per second. For overflow attacks, the threshold is the buffer size for the command. For large ICMP attacks, the threshold is the ICMP packet size limit to pass through.

For example, setting the icmpflood signature threshold to 500 will allow 500 echo requests from a source address, to which the system sends echo replies. If the number of requests is 501 or higher, the FortiGate unit will block the attacker to eliminate disruption of system operations.

If you enter a threshold value of 0 or a number out of the allowable range, the FortiGate unit uses the default value.

**Table 6: NIDS Prevention signatures with threshold values**

| Signature abbreviation | Threshold value units                                                                                  | Default threshold value | Minimum threshold value | Maximum threshold value |
|------------------------|--------------------------------------------------------------------------------------------------------|-------------------------|-------------------------|-------------------------|
| synflood               | Maximum number of SYN segments received per second                                                     | 200                     | 30                      | 3000                    |
| portscan               | Maximum number of SYN segments received per second                                                     | 128                     | 10                      | 256                     |
| srcsession             | Total number of TCP sessions initiated from the same source                                            | 2048                    | 128                     | 10240                   |
| ftpvfl                 | Maximum buffer size for an FTP command (bytes)                                                         | 256                     | 128                     | 1024                    |
| smtpvfl                | Maximum buffer size for an SMTP command (bytes)                                                        | 512                     | 128                     | 1024                    |
| pop3ovfl               | Maximum buffer size for a POP3 command (bytes)                                                         | 512                     | 128                     | 1024                    |
| udpflood               | Maximum number of UDP packets received from the same source or sent to the same destination per second | 2048                    | 512                     | 102400                  |
| udpsrcsession          | Total number of UDP sessions initiated from the same source                                            | 1024                    | 512                     | 102400                  |
| icmpflood              | Maximum number of UDP packets received from the same source or sent to the same destination per second | 256                     | 128                     | 102400                  |
| icmpsrcsession         | Total number of ICMP sessions initiated from the same source                                           | 128                     | 64                      | 2048                    |
| icmpsweep              | Maximum number of ICMP packets received from the same source per second                                | 32                      | 16                      | 2048                    |
| icmplarge              | Maximum ICMP packet size (bytes)                                                                       | 32000                   | 1024                    | 64000                   |

To set Prevention signature threshold values:

- 1 Go to **NIDS > Prevention**.
- 2 Select Modify  beside the signature for which you want to set the Threshold value.  
Signatures that do not have threshold values do not have Modify  icons.
- 3 Type the Threshold value.
- 4 Select the Enable check box.
- 5 Select OK.

## Configuring synflood signature values

For synflood signatures, you can set the threshold, queue size, and keep alive values.

| Value      | Description                                                                                                                                                                                              | Minimum value | Maximum value | Default value |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|---------------|---------------|
| Threshold  | Number of SYN requests sent to a destination host or server per second. If the SYN requests are being sent to all ports on the destination, as opposed to just one port, the threshold quadruples (4 x). | 30            | 3000          | 200           |
| Queue Size | Maximum number of proxied connections that the FortiGate unit handles. The FortiGate unit discards additional proxy requests.                                                                            | 10            | 10240         | 1024          |
| Timeout    | Number of seconds for the SYN cookie to keep a proxied connection alive. This value limits the size of the proxy connection table.                                                                       | 3             | 60            | 15            |

- 1 Go to **NIDS > Prevention**.
- 2 Select Modify  for the synflood signature.
- 3 Type the Threshold value.
- 4 Type the Queue Size.
- 5 Type the Timeout value.
- 6 Select the Enable check box.  
Alternatively, select the synflood Enable check box in the Prevention signature list.
- 7 Select OK.

## Logging attacks

Whenever the NIDS detects or prevents an attack, it generates an attack message. You can configure the system to add the message to the attack log.

- [Logging attack messages to the attack log](#)
- [Reducing the number of NIDS attack log and email messages](#)

### Logging attack messages to the attack log

Use the following procedure to log attack messages to the attack log.

- 1 Go to **Log&Report > Log Setting**.
- 2 Select Config Policy for the log locations you have set.
- 3 Select Attack Log.
- 4 Select Attack Detection and Attack Prevention.
- 5 Select OK.



**Note:** For information about log message content and formats, and about log locations, see the *Logging Configuration and Reference Guide*.

## Reducing the number of NIDS attack log and email messages

Intrusion attempts may generate an excessive number of attack messages. To help you distinguish real warnings from false alarms, the FortiGate unit provides methods to reduce the number of unnecessary messages. Based on the frequency that messages are generated, the FortiGate unit will automatically delete duplicates. If you determine that you are still receiving an excessive number of unnecessary messages, you can manually disable message generation for signature groups.

### Automatic message reduction

The content of the attack log and alert email messages that the NIDS produces includes the ID number and name of the attack that generated the message. The attack ID number and name in the message are identical to the ID number and rule name that appear on the NIDS Signature Group Members list.

The FortiGate unit uses an alert email queue in which each new message is compared with the previous messages. If the new message is not a duplicate, the FortiGate unit sends it immediately and puts a copy in the queue. If the new message is a duplicate, the FortiGate unit deletes it and increases an internal counter for the number of message copies in the queue.

The FortiGate unit holds duplicate alert email messages for 60 seconds. If a duplicate message has been in the queue for more than 60 seconds, the FortiGate unit deletes the message and increases the copy number. If the copy number is greater than 1, the FortiGate unit sends a summary email that includes “Repeated x times” in the subject header, the statement “The following email has been repeated x times in the last y seconds”, and the original message.

### Manual message reduction

If you want to reduce the number of alerts that the NIDS generates, you can review the content of attack log messages and alert email. If a large number of the alerts are nuisance alerts (for example, web attacks when you are not running a web server), you can disable the signature group for that attack type. Use the ID number in the attack log or alert email to locate the attack in the signature group list. See [“Enabling and disabling NIDS attack signatures” on page 224](#).



# Antivirus protection

Antivirus protection is enabled in firewall policies. When you enable antivirus protection for a firewall policy, you select a content profile that controls how the antivirus protection behaves. Content profiles control the type of traffic protected (HTTP, FTP, IMAP, POP3, SMTP), the type of antivirus protection and the treatment of fragmented email and oversized files or email.

This chapter describes:

- [General configuration steps](#)
- [Antivirus scanning](#)
- [File blocking](#)
- [Blocking oversized files and emails](#)
- [Exempting fragmented email from blocking](#)
- [Viewing the virus list](#)

## General configuration steps

Configuring antivirus protection involves the following general steps.

- 1 Select antivirus protection options in a new or existing content profile. See [“Adding a content profile” on page 170](#).
- 2 Select the Anti-Virus & Web filter option in firewall policies that allow web (HTTP), FTP, and email (IMAP, POP3, and SMTP) connections through the FortiGate unit. Select a content profile that provides the antivirus protection options that you want to apply to a policy. See [“Adding a content profile to a policy” on page 171](#).
- 3 Configure antivirus protection settings to control how the FortiGate unit applies antivirus protection to the web, FTP, and email traffic allowed by policies. See:
  - [“Antivirus scanning” on page 232](#),
  - [“File blocking” on page 233](#),
  - [“Blocking oversized files and emails” on page 234](#),
  - [“Exempting fragmented email from blocking” on page 234](#).
- 4 Configure the messages that users receive when the FortiGate unit blocks or deletes an infected file. See [“Customizing replacement messages” on page 136](#).
- 5 Configure the FortiGate unit to send an alert email when it blocks or deletes an infected file. See [“Configuring alert email” in the \*Logging and Message Reference Guide\*](#).



**Note:** To receive virus log messages, see [“Configuring logging”](#), and for information about log message content and format, see [“Virus log messages” in the \*Logging Configuration and Reference Guide\*](#)

## Antivirus scanning

Virus scanning intercepts most files (including files compressed with up to 12 layers of compression using zip, rar, gzip, tar, upx, and OLE) in the content streams for which antivirus protection has been enabled. Each file is tested to determine the file type and to determine the most effective method of scanning the file for viruses. For example, binary files are scanned using binary virus scanning and Microsoft Office files containing macros are scanned for macro viruses.

FortiGate virus scanning does not scan the following file types:

- cdimage
- floppy image
- .ace
- .bzip2
- .Tar+Gzip+Bzip2

If a file is found to contain a virus it is removed from the content stream and replaced with a replacement message.

### To scan FortiGate firewall traffic for viruses

- 1 Select antivirus scanning in a content profile.  
See [“Adding a content profile” on page 170](#).
- 2 Add this content profile to firewall policies to apply virus scanning to the traffic controlled by the firewall policy.  
See [“Adding a content profile to a policy” on page 171](#).

Figure 37: Example content profile for virus scanning

Content Profile

New Content Profile

Profile Name:

| Options                | HTTP                                                                 | FTP                                                                  | IMAP                                                                 | POP3                                                                 | SMTP                                                                 |
|------------------------|----------------------------------------------------------------------|----------------------------------------------------------------------|----------------------------------------------------------------------|----------------------------------------------------------------------|----------------------------------------------------------------------|
| Anti Virus Scan        | <input checked="" type="checkbox"/>                                  | <input checked="" type="checkbox"/>                                  | <input checked="" type="checkbox"/>                                  | <input checked="" type="checkbox"/>                                  | <input checked="" type="checkbox"/>                                  |
| File Block             | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             |
| Web URL Block          | <input type="checkbox"/>                                             |                                                                      |                                                                      |                                                                      |                                                                      |
| Web Content Block      | <input type="checkbox"/>                                             |                                                                      |                                                                      |                                                                      |                                                                      |
| Web Script Filter      | <input type="checkbox"/>                                             |                                                                      |                                                                      |                                                                      |                                                                      |
| Web Exempt List        | <input type="checkbox"/>                                             |                                                                      |                                                                      |                                                                      |                                                                      |
| Email Block List       |                                                                      |                                                                      | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             |                                                                      |
| Email Exempt List      |                                                                      |                                                                      | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             |                                                                      |
| Email Content Block    |                                                                      |                                                                      | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             |                                                                      |
| Oversized File/Email   | <input type="radio"/> block<br><input checked="" type="radio"/> pass | <input type="radio"/> block<br><input checked="" type="radio"/> pass | <input type="radio"/> block<br><input checked="" type="radio"/> pass | <input type="radio"/> block<br><input checked="" type="radio"/> pass | <input type="radio"/> block<br><input checked="" type="radio"/> pass |
| Pass Fragmented Emails |                                                                      |                                                                      | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             | <input type="checkbox"/>                                             |

OK Cancel

## File blocking

Enable file blocking to remove all files that pose a potential threat and to provide the best protection from active computer virus attacks. Blocking files is the only protection available from a virus that is so new that antivirus scanning cannot detect it. You would not normally run the FortiGate unit with blocking enabled. However, it is available for extremely high-risk situations in which there is no other way to prevent viruses from entering your network.

File blocking deletes all files that match a list of enabled file patterns. The FortiGate unit replaces the file with an alert message that is forwarded to the user. The FortiGate unit also writes a message to the virus log and sends an alert email if it is configured to do so.



**Note:** If both blocking and scanning are enabled, the FortiGate unit blocks files that match enabled file patterns and does not scan these files for viruses.

By default, when blocking is enabled, the FortiGate unit blocks the following file patterns:

- executable files (\*.bat, \*.com, and \*.exe)
- compressed or archive files (\*.gz, \*.rar, \*.tar, \*.tgz, and \*.zip)
- dynamic link libraries (\*.dll)
- HTML application (\*.hta)
- Microsoft Office files (\*.doc, \*.ppt, \*.xl?)
- Microsoft Works files (\*.wps)
- Visual Basic files (\*.vb?)
- screen saver files (\*.scr)

### Blocking files in firewall traffic

Use content profiles to apply file blocking to HTTP, FTP, POP3, IMAP, and SMTP traffic controlled by firewall policies.

- 1 Select file blocking in a content profile.  
See [“Adding a content profile” on page 170](#).
- 2 Add this content profile to firewall policies to apply content blocking to the traffic controlled by the firewall policy.  
See [“Adding a content profile to a policy” on page 171](#).

### Adding file patterns to block

- 1 Go to **Anti-Virus > File Block**.
- 2 Select New.
- 3 Type the new pattern in the File Pattern field.  
You can use an asterisk (\*) to represent any characters and a question mark (?) to represent any single character. For example, \*.dot blocks Microsoft Word template files and \*.do? blocks both Microsoft Word template files and document files.
- 4 Select the check box beside the traffic protocols for which you want to enable blocking of this file pattern.
- 5 Select OK.

## Blocking oversized files and emails

You can configure the FortiGate unit to buffer 1 to 15 percent of available memory to store oversized files and email. The FortiGate unit then blocks a file or email that exceeds this limit instead of bypassing antivirus scanning and sending the file or email directly to the server or receiver. The FortiGate unit sends a replacement message for an oversized file or email attachment to the HTTP or email proxy client.

### Configuring limits for oversized files and email

- 1 Go to **Anti-Virus > Config > Config**.
- 2 Type the size limit in MB.
- 3 Select Apply.

## Exempting fragmented email from blocking

A fragmented email is a large email message that has been split into smaller messages that are sent individually and recombined when they are received. By default when antivirus protection is enabled, the FortiGate unit blocks fragmented emails and replaces them with an email block message that is forwarded to the receiver. It is recommend that you disable the fragmenting of email messages in the client email software.

To exempt fragmented emails from automatic antivirus blocking, you can enable Pass Fragmented Email for the email content protocols (IMAP, POP3, and SMTP).



**Caution:** The FortiGate unit cannot scan fragmented emails for viruses or use file pattern blocking to remove files from these email messages.

Configure the FortiGate unit to pass fragmented emails by doing the following:

- 1 Enable Pass Fragmented Emails for IMAP, POP3, and SMTP traffic in a content profile.
- 2 Select Anti-Virus & Web filter in a firewall policy. For example, to pass fragmented emails that internal users send to the external network, select an internal to external policy.
- 3 Select a content profile that has Pass Fragmented Emails enabled for the traffic that you want the FortiGate unit to scan.

## Viewing the virus list

Use the following procedure to view the names of the viruses and worms in the current virus definition list:

- 1 To display the virus list, go to **Anti-Virus > Config > Virus List**.
- 2 Scroll through the virus and worm list to view the names of all viruses and worms in the list.

# Web filtering

Web filtering is enabled in firewall policies. When you enable Anti-Virus & Web filter in a firewall policy, you select a content profile that controls how web filtering behaves for HTTP traffic. Content profiles control the following types of content filtering:

- blocking unwanted URLs,
- blocking unwanted content,
- removing scripts from web pages,
- exempting of URLs from blocking.

You can also use the Cerberian URL blocking to block unwanted URLs. For more information, see [“Using the Cerberian web filter” on page 240](#).

This chapter describes:

- [General configuration steps](#)
- [Content blocking](#)
- [URL blocking](#)
- [Using the Cerberian web filter](#)
- [Script filtering](#)
- [Exempt URL list](#)

## General configuration steps

Configuring web filtering involves the following general steps:

- 1 Select web filtering options in a new or existing content profile. See [“Adding a content profile” on page 170](#).
- 2 Select the Anti-Virus & Web filter option in firewall policies that allow HTTP connections through the FortiGate unit.
  - Select a content profile that provides the web filtering options that you want to apply to a policy. See [“Adding a content profile to a policy” on page 171](#).
- 3 Configure web filtering settings to control how the FortiGate unit applies web filtering to the HTTP traffic allowed by policies. See:
  - [“URL blocking” on page 237](#),
  - [“Using the Cerberian web filter” on page 240](#),
  - [“Content blocking” on page 236](#),
  - [“Script filtering” on page 242](#),
  - [“Exempt URL list” on page 243](#).

- 4 Configure the messages that users receive when the FortiGate unit blocks unwanted content or unwanted URLs. See [“Customizing replacement messages” on page 136](#).
- 5 Configure the FortiGate unit to send an alert email when it blocks or deletes an infected file. See “Configuring alert email” in the *Logging Configuration and Reference Guide*.



**Note:** To receive web filtering log messages, see “Configuring logging”, and for information about log message content and format, see “Web filtering log messages” in the *Logging Configuration and Reference Guide*.

## Content blocking

When the FortiGate unit blocks a web page, the user who requested the blocked page receives a block message and the FortiGate unit writes a message to the web filtering log.

You can add banned words to the list in many languages using Western, Simplified Chinese, Traditional Chinese, Japanese, or Korean character sets.

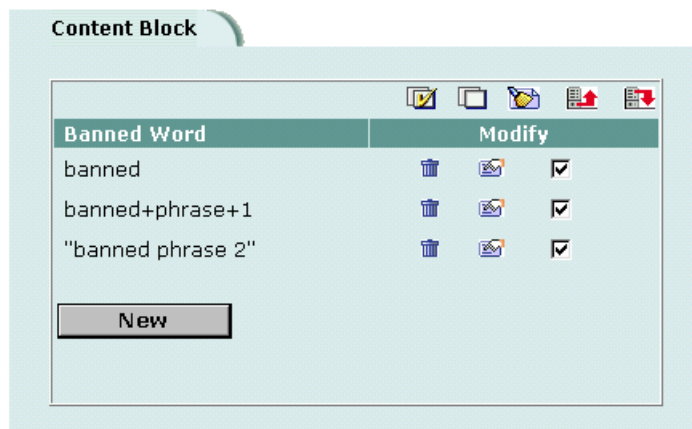
### Adding words and phrases to the banned word list

- 1 Go to **Web Filter > Content Block**.
- 2 Select New to add a word or phrase to the banned word list.
- 3 Choose a language or character set for the banned word or phrase.  
You can choose Western, Chinese Simplified, Chinese Traditional, Japanese, or Korean.  
Your computer and web browser must be configured to enter characters in the character set that you choose.
- 4 Type a banned word or phrase.  
If you type a single word (for example, banned), the FortiGate unit blocks all web pages that contain that word.  
If you type a phrase (for example, banned phrase), the FortiGate unit blocks web pages that contain both words. When this phrase appears on the banned word list, the FortiGate unit inserts plus signs (+) in place of spaces (for example, banned+phrase).  
If you type a phrase in quotes (for example, “banned word”), the FortiGate unit blocks all web pages in which the words are found together as a phrase.  
Content filtering is not case-sensitive. You cannot include special characters in banned words.
- 5 Select OK.  
The word or phrase is added to the banned word list.
- 6 In the Modify column, check the box beside the new item in the banned word list so that the FortiGate unit blocks web pages containing this word or phrase.  
You can enter multiple banned words or phrases and then select Check All  to activate all items in the banned word list.



**Note:** Banned Word must be selected in the content profile for web pages containing banned words to be blocked.

Figure 38: Example banned word list



## URL blocking

You can block the unwanted web URLs using both the FortiGate web filter and the Cerberian web filter.

- [Using the FortiGate web filter](#)
- [Using the Cerberian web filter](#)

### Using the FortiGate web filter

You can configure the FortiGate unit to block all pages on a website by adding the top-level URL or IP address. You can also block individual pages on a website by including the full path and filename of the web page to block.

This section describes:

- [Adding URLs or URL patterns to the block list](#)
- [Clearing the URL block list](#)
- [Downloading the URL block list](#)
- [Uploading a URL block list](#)

### Adding URLs or URL patterns to the block list

- 1 Go to **Web Filter > URL Block**.
- 2 Select **New** to add an item to the URL block list.

### 3 Type the URL/Pattern to block.

Type a top-level URL or IP address to block access to all pages on a website. For example, `www.badsite.com` or `122.133.144.155` blocks access to all pages at this website.

Type a top-level URL followed by the path and filename to block access to a single page on a website. For example, `www.badsite.com/news.html` or `122.133.144.155/news.html` blocks the news page on this website.

To block all pages with a URL that ends with `badsite.com`, add `badsite.com` to the block list. For example, adding `badsite.com` blocks access to `www.badsite.com`, `mail.badsite.com`, `www.finance.badsite.com`, and so on.



**Note:** Do not include `http://` in the URL to block. Do not use an asterisk (\*) to represent any characters. You can type a top-level domain suffix (for example, “com” without the leading period) to block access to all URLs with this suffix.



**Note:** URL blocking does not block access to other services that users can access with a web browser. For example, URL blocking does not block access to `ftp://ftp.badsite.com`. Instead, you can use firewall policies to deny FTP connections.

### 4 Select Enable to block the URL/Pattern.

### 5 Select OK to add the URL/Pattern to the URL block list.

You can enter multiple URLs and patterns and then select Check All  to enable all items in the URL block list.

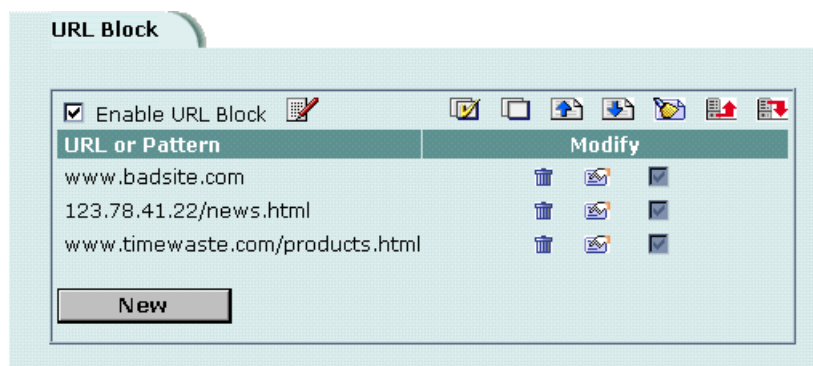
Each page of the URL block list displays 100 URLs.

### 6 Use Page Up and Page Down to navigate through the URL block list.



**Note:** You must select the Web URL Block option in the content profile to enable the URL blocking.

**Figure 39: Example URL block list**



## Clearing the URL block list

### 1 Go to **Web Filter > URL Block**.

### 2 Select Clear URL Block List to remove all URLs and patterns from the URL block list.

## Downloading the URL block list

You can back up the URL block list by downloading it to a text file on the management computer.

- 1 Go to **Web Filter > URL Block**.
- 2 Select Download URL Block List .

The FortiGate unit downloads the list to a text file on the management computer. You can specify a location to which to download the text file as well as a name for the text file.

## Uploading a URL block list

You can create a URL block list in a text editor and then upload the text file to the FortiGate unit. Add one URL or pattern to each line of the text file. You can follow the item with a space and then a 1 to enable or a zero (0) to disable the URL. If you do not add this information to the text file, the FortiGate unit automatically enables all URLs and patterns that are followed with a 1 or no number when you upload the text file.

**Figure 40: Example URL block list text file**

```
www.badsite.com/index 1
www.badsite.com/products 1
182.63.44.67/index 1
```

You can either create the URL block list yourself or add a URL list created by a third-party URL block or blacklist service. For example, you can download the squidGuard blacklists available at <http://www.squidguard.org/blacklist/> as a starting point for creating your own URL block list. Three times per week, the squidGuard robot searches the web for new URLs to add to the blacklists. You can upload the squidGuard blacklists to the FortiGate unit as a text file, with only minimal editing to remove comments at the top of each list and to combine the lists that you want into a single file.



**Note:** All changes made to the URL block list using the web-based manager are lost when you upload a new list. However, you can download your current URL block list, add more items to it using a text editor, and then upload the edited list to the FortiGate unit.

- 1 In a text editor, create the list of URLs and patterns to block.
- 2 Using the web-based manager, go to **Web Filter > URL Block**.
- 3 Select Upload URL Block List .
- 4 Type the path and filename of your URL block list text file, or select Browse and locate the file.
- 5 Select OK to upload the file to the FortiGate unit.
- 6 Select Return to display the updated URL block list.  
Each page of the URL block list displays 100 URLs.
- 7 Use Page Down  and Page Up  to navigate through the URL block list.
- 8 You can continue to maintain the URL block list by making changes to the text file and uploading it again.

## Using the Cerberian web filter

The FortiGate unit supports Cerberian web filtering. For information about Cerberian web filter, see [www.cerberian.com](http://www.cerberian.com).

If you have purchased the Cerberian web filtering functionality with your FortiGate unit, use the following configuration procedures to configure FortiGate support for Cerberian web filtering.

### General configuration steps

To use the Cerberian web filter, you must:

- 1 Install a Cerberian web filter license key. See [“Installing a Cerberian license key on the FortiGate unit” on page 240](#).
- 2 Add users that will be using the Cerberian web filter. See [“Adding a Cerberian user to the FortiGate unit” on page 240](#).
- 3 Configure the Cerberian web filter. See [“Using the Cerberian web filter” on page 240](#).
- 4 Enable Cerberian URL filtering. See [“Using the Cerberian web filter” on page 240](#).



**Note:** To use Cerberian web filtering, the FortiGate unit must have access to the Internet.

### Installing a Cerberian license key on the FortiGate unit

Before you can use the Cerberian web filter, you must install a license key. The license key determines the number of end users allowed to use Cerberian web filtering through the FortiGate unit.

- 1 Go to **Web Filter > URL Block**.
- 2 Select Cerberian URL Filtering.
- 3 Enter the license number.
- 4 Select Apply.

### Adding a Cerberian user to the FortiGate unit

The Cerberian web policies can only be applied to user groups. You can add users on the FortiGate unit and then add the users to user groups on the Cerberian administration web site.

When the end user tries to access a URL, the FortiGate unit will check to see if the user's IP address is in the IP address list on the FortiGate unit. If the user's IP address is in the list, the request will be sent to the Cerberian server. Otherwise, an error message will be sent to the user saying that the user doesn't have authorized access to the Cerberian web filter.

- 1 Go to **Web Filter > URL Block**.
- 2 Select Cerberian URL Filtering.
- 3 Select New.

- 4 Enter the IP address and netmask of the user computers. You can enter the IP address of a single user. For example, 192.168.100.19 255.255.255.255. You can also enter a subnet of a group of users. For example, 192.168.100.0 255.255.255.0.
- 5 Enter an alias for the user. This alias will be used as the user name when you add the user to a user group on the Cerberian server. If you do not enter an alias, the user's IP will be used and added to the default group on the Cerberian server.
- 6 Select OK.

## Configuring Cerberian web filter

After you add the Cerberian web filter users on the FortiGate unit, you can add the users to the user groups on the Cerberian web filter server. Then you can create policies and apply the policies to the user groups.

### About the default group and policy

There is a default user group, which is associated with a default policy, existing on the Cerberian web filter.

You can add users to the default group and apply any policies to the group.

The default group is a place for:

- All the users who are not assigned alias names on the FortiGate unit.
- All the users who are not assigned to any other user groups.

The Cerberian web filter groups the web pages into 53 categories. The default policy blocks the URLs of 12 categories. You can modify the default policy and apply it to any user groups.

### To configure the Cerberian web filtering

- 1 Add the user name, which is the alias you added on the FortiGate unit, to a user group on the Cerberian server because the web policies can only be applied to the user groups. If you did not enter an alias for the user IP on the FortiGate unit, the user IP is automatically added to the default group.
- 2 Create your policies by selecting the web categories that you want to block.
- 3 Apply the policy to a user group which contains the user.

For detailed procedures, see the online help on the Cerberian Web Filter web page.

## Enabling Cerberian URL filtering

After you add the Cerberian users/groups and configure the Cerberian web filter, you can enable Cerberian URL filtering. You must enable it in three places:

- The Cerberian URL Filtering page.
- The content profile.
- The policy that uses the content profile.

- 1 Go to **Web Filter > URL Block**.
- 2 Select Cerberian URL Filtering.
- 3 Select the Cerberian URL Filtering option.
- 4 Go to **Firewall > Content Profile**.

- 5 Create a new or select an existing content profile and enable Web URL Block.
- 6 Go to **Firewall > Policy**.
- 7 Create a new or select an existing policy that will use the content profile.
- 8 Select Anti-Virus & Web filter.
- 9 Select the content profile from the Content Profile list.
- 10 Click OK.

## Script filtering

You can configure the FortiGate unit to remove Java applets, cookies, and ActiveX scripts from the HTML web pages.



**Note:** Blocking of any of these items might prevent some web pages from working properly.

- [Enabling the script filter](#)
- [Selecting script filter options](#)

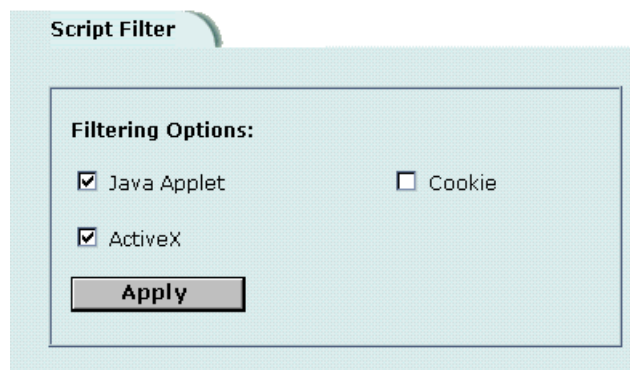
### Enabling the script filter

- 1 Go to **Firewall > Content Profile**.
- 2 Select the content profile for which you want to enable script filtering.
- 3 Select Script Filter.
- 4 Select OK.

### Selecting script filter options

- 1 Go to **Web Filter > Script Filter**.
- 2 Select the script filter options that you want to enable.  
You can block Java applets, cookies, and ActiveX.
- 3 Select Apply.

**Figure 41:** Example script filter settings to block Java applets and ActiveX



## Exempt URL list

Add URLs to the exempt URL list to allow legitimate traffic that might otherwise be blocked by content or URL blocking. For example, if content blocking is set to block pornography-related words and a reputable website runs a story on pornography, web pages from the reputable website would be blocked. Adding the address of the reputable website to the exempt URL list allows the content of the website to bypass content blocking.

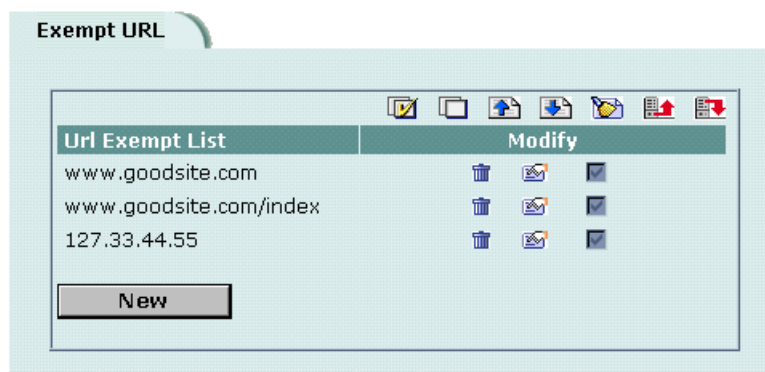


**Note:** Content downloaded from exempt web pages is not blocked or scanned by antivirus protection.

### Adding URLs to the exempt URL list

- 1 Go to **Web Filter > Exempt URL**.
- 2 Select New to add an item to the exempt URL list.
- 3 Type the URL to exempt.  
Type a complete URL, including path and filename, to exempt access to a page on a website. For example, `www.goodsite.com/index.html` exempts access to the main page of this example website. You can also add IP addresses; for example, `122.63.44.67/index.html` exempts access to the main web page at this address. Do not include `http://` in the URL to exempt.  
Exempting a top-level URL, such as `www.goodsite.com`, exempts all requested subpages (for example, `www.goodsite.com/badpage`) from all content and URL filtering rules.
- 4 Select Enable to exempt the URL.
- 5 Select OK to add the URL to the exempt URL list.  
You can enter multiple URLs and then select Check All  to activate all items in the exempt URL list.  
Each page of the exempt URL list displays 100 URLs.
- 6 Use Page Down  and Page Up  to navigate through the exempt URL list.

**Figure 42: Example exempt URL list**





# Email filter

Email filtering is enabled in firewall policies. When you enable Anti-Virus & Web filter in a firewall policy, you select a content profile that controls how email filtering behaves for email (IMAP and POP3) traffic. Content profiles control the following types of protection to identify unwanted email:

- filtering of unwanted sender address patterns,
- filtering of unwanted content,
- exempting sender address patterns from blocking.

This chapter describes:

- [General configuration steps](#)
- [Email banned word list](#)
- [Email block list](#)
- [Email exempt list](#)
- [Adding a subject tag](#)

## General configuration steps

Configuring email filtering involves the following general steps:

- 1 Select email filter options in a new or existing content profile. See [“Adding a content profile” on page 170](#).
- 2 Select the Anti-Virus & Web filter option in firewall policies that allow IMAP and POP3 connections through the FortiGate unit. Select a content profile that provides the email filtering options that you want to apply to a policy. See [“Adding a content profile to a policy” on page 171](#).
- 3 Add a subject tag to the unwanted email so that receivers can use their mail client software to filter messages based on the tag. See [“Adding a subject tag” on page 248](#).



**Note:** To receive email filter log messages, see “Configuring logging” in the *Logging Configuration and Reference Guide*. For information about email filter log message categories and formats, see “Log messages” in the *FortiGate Logging Configuration and Reference Guide*.

## Email banned word list

When the FortiGate unit detects email that contains a word or phrase in the banned word list, the FortiGate unit adds a tag to the subject line of the email and writes a message to the event log. Receivers can then use their mail client software to filter messages based on the subject tag.

You can add banned words to the list in many languages using Western, Simplified Chinese, Traditional Chinese, Japanese, or Korean character sets.

### Adding words and phrases to the banned word list

- 1 Go to **Email Filter > Content Block**.
- 2 Select New to add a word or phrase to the banned word list.
- 3 Type a banned word or phrase.
  - If you type a single word (for example, banned), the FortiGate unit tags all IMAP and POP3 email that contains that word.
  - If you type a phrase (for example, banned phrase), the FortiGate unit tags email that contains both words. When this phrase appears on the banned word list, the FortiGate unit inserts plus signs (+) in place of spaces (for example, banned+phrase).
  - If you type a phrase in quotes (for example, "banned word"), the FortiGate unit tags all email in which the words are found together as a phrase.

Content filtering is not case-sensitive. You cannot include special characters in banned words.

- 4 Select the Language for the banned word or phrase.

You can choose Western, Chinese Simplified, Chinese Traditional, Japanese, or Korean.

Your computer and web browser must be configured to enter characters in the language that you select.
- 5 Select Enable.
- 6 Select OK.

The word or phrase is added to the banned word list.

You can enter multiple banned words or phrases and then select Check All  to activate all items in the banned word list.



**Note:** Email Content Block must be selected in the content profile for IMAP or POP3 email containing banned words to be tagged.

## Email block list

You can configure the FortiGate unit to tag all IMAP and POP3 protocol traffic sent from unwanted email addresses. When the FortiGate unit detects an email sent from an unwanted address pattern, the FortiGate unit adds a tag to the subject line of the email and writes a message to the email filter log. Receivers can then use their mail client software to filter messages based on the subject tag.

You can tag email from a specific sender address or from all address subdomains by adding the top-level domain name. Alternatively, you can tag email sent from individual subdomains by including the subdomain to block.

### Adding address patterns to the email block list

- 1 Go to **Email Filter > Block List**.
- 2 Select **New** to add an address pattern to the Email Block list.
- 3 Type a Block Pattern.
  - To tag email from a specific email address, type the email address. For example, `sender@abccompany.com`.
  - To tag email from a specific domain, type the domain name. For example, `abccompany.com`.
  - To tag email from a specific subdomain, type the subdomain name. For example, `mail.abccompany.com`.
  - To tag email from an entire organization category, type the top-level domain name. For example, type `com` to tag email sent from all organizations that use `.com` as the top-level domain.

The pattern can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - (hyphen), \_ (underscore), and @. Spaces and other special characters are not allowed.

- 4 Select **Enable** to tag the email if part or all of the email address match the block pattern.
- 5 Select **OK** to add the address pattern to the Email Block list.

You can enter multiple address patterns and then select **Check All**  to enable all patterns in the Email Block list.

You can also enable any pattern in the Email Block list by checking the box in the **Enable** column.

## Email exempt list

Add address patterns to the exempt list to allow legitimate IMAP and POP3 traffic that might otherwise be tagged by email or content blocking. For example, if the email banned word list is set to block email that contains pornography-related words and a reputable company sends email that contains these words, the FortiGate unit would normally add a subject tag to the email. Adding the domain name of the reputable company to the exempt list allows IMAP and POP3 traffic from the company to bypass email and content blocking.

## Adding address patterns to the email exempt list

- 1 Go to **Email Filter > Exempt List**.
- 2 Select New to add an address pattern to the email exempt list.
- 3 Type the address pattern to exempt.
  - To exempt email sent from a specific email address, type the email address. For example, sender@abccompany.com.
  - To exempt email sent from a specific domain, type the domain name. For example, abccompany.com.
  - To exempt email sent from a specific subdomain, type the subdomain name. For example, mail.abccompany.com.
  - To exempt email sent from an entire organization category, type the top-level domain name. For example, type net to exempt email sent from all organizations that use .net as the top-level domain.

The pattern can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - (hyphen), \_ (underscore), and @. Spaces and other special characters are not allowed.
- 4 Select Enable to exempt the address pattern.
- 5 Select OK to add the address pattern to the email exempt list.

You can enter multiple patterns and then select Check All  to activate all patterns in the email exempt list.

You can also enable any pattern in the email exempt list by checking the box in the Enable column.

## Adding a subject tag

When the FortiGate unit receives email from an unwanted address or email that contains an item in the email banned word list, the FortiGate unit adds a tag to the subject line and sends the message to the destination email address. Email users can use their mail client software to filter the messages based on the subject tag.

### To add a subject tag

- 1 Go to **Email Filter > Config**.
- 2 Type the Subject Tag that you want to display in the subject line of email received from unwanted addresses or that contains banned words. For example, type Unwanted Mail.



**Note:** Do not use quotation marks in the subject tags.

- 3 Select Apply.

The FortiGate unit adds the tag to the subject line of all unwanted email.

# Logging and reporting

You can configure the FortiGate unit to log network activity from routine configuration changes and traffic sessions to emergency events. You can also configure the FortiGate unit to send alert email messages to inform system administrators about events such as network attacks, virus incidents, and firewall and VPN events.

This chapter describes:

- [Recording logs](#)
- [Filtering log messages](#)
- [Configuring traffic logging](#)
- [Viewing logs saved to memory](#)
- [Configuring alert email](#)

## Recording logs

You can configure logging to record logs to one or more of:

- a computer running a syslog server,
- a computer running a WebTrends firewall reporting server,
- the console.

You can also configure logging to record event, attack, antivirus, web filter, and email filter logs to the FortiGate system memory if your FortiGate unit does not contain a hard disk. Logging to memory allows quick access to only the most recent log entries. If the FortiGate unit restarts, the log entries are lost.

You can select the same or different severity levels for each log location. For example, you might want to record only emergency and alert level messages to the FortiGate memory and record all levels of messages on a remote computer.

For information about filtering the log types and activities that the FortiGate unit records, see [“Filtering log messages” on page 251](#). For information about traffic logs, see [“Configuring traffic logging” on page 253](#).

This section describes:

- [Recording logs on a remote computer](#)
- [Recording logs on a NetIQ WebTrends server](#)
- [Recording logs in system memory](#)

## Recording logs on a remote computer

Use the following procedure to configure the FortiGate unit to record log messages on a remote computer. The remote computer must be configured with a syslog server.

- 1 Go to **Log&Report > Log Setting**.
- 2 Select Log to Remote Host to send the logs to a syslog server.
- 3 Type the IP address of the remote computer running syslog server software.
- 4 Type the port number of the syslog server.
- 5 Select the severity level for which you want to record log messages.  
The FortiGate will log all levels of severity down to but not lower than the level you choose. For example, if you want to record emergency, alert, critical, and error messages, select Error.
- 6 Select Config Policy.
  - Select the Log type for which you want the FortiGate unit to record logs.
  - For each Log type, select the activities for which you want the FortiGate unit to record log messages.
  - Select OK.For more information on log types and activities, see [“Filtering log messages” on page 251](#) and [“Configuring traffic logging” on page 253](#).
- 7 Select Apply.

## Recording logs on a NetIQ WebTrends server

Use the following procedure to configure the FortiGate unit to record logs on a remote NetIQ WebTrends firewall reporting server for storage and analysis. FortiGate log formats comply with WebTrends Enhanced Log Format (WELF) and are compatible with WebTrends NetIQ Security Reporting Center 2.0 and Firewall Suite 4.1. See the Security Reporting Center and Firewall Suite documentation for more information.



**Note:** FortiGate traffic log messages include sent and received fields, which are optional but required for drawing a WebTrends graph.

To record logs on a NetIQ WebTrends server:

- 1 Go to **Log&Report > Log Setting**.
- 2 Select Log in WebTrends Enhanced Log Format.
- 3 Type the IP address of the NetIQ WebTrends firewall reporting server.
- 4 Select the severity level for which you want to record log messages.  
The FortiGate will log all levels of severity down to but not lower than the level you choose. For example, if you want to record emergency, alert, critical, and error messages, select Error.
- 5 Select Config Policy.  
To configure the FortiGate to filter the types of logs and events to record, use the procedures in [“Filtering log messages” on page 251](#) and [“Configuring traffic logging” on page 253](#).
- 6 Select Apply.

## Recording logs in system memory

If your FortiGate unit does not contain a hard disk, you can use the following procedure to configure the FortiGate unit to reserve some system memory for storing current event, attack, antivirus, web filter and email filter log messages. Logging to memory allows quick access to only the most recent log entries. The FortiGate unit can store a limited number of messages in system memory. After all available memory is used, the FortiGate unit deletes the oldest messages. If the FortiGate unit restarts, the log entries are lost.



**Note:** The FortiGate unit can only record the event and attack log messages in system memory.

To record logs in system memory:

- 1 Go to **Log&Report > Log Setting**.
- 2 Select Log to memory.
- 3 Select the severity level for which you want to record log messages.  
The FortiGate will log all levels of severity down to but not lower than the level you choose. For example, if you want to record emergency, alert, critical, and error messages, select Error.
- 4 Select Config Policy.  
To configure the FortiGate to filter the types of logs and events to record, use the procedures in [“Filtering log messages” on page 251](#).
- 5 Select Apply.

## Filtering log messages

You can configure which logs to record and which message categories to record in each log.

- 1 Go to **Log&Report > Log Setting**.
- 2 Select Config Policy for the log location that you selected in [“Recording logs” on page 249](#).
- 3 Select the log types that you want FortiGate unit to record.

|                          |                                                                                                                                                                                                                                                                                    |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Traffic Log</b>       | Record all connections to and through the interface.<br>To configure traffic filtering, see <a href="#">“Adding traffic filter entries” on page 254</a> .                                                                                                                          |
| <b>Event Log</b>         | Record management and activity events in the event log.<br>Management events include changes to the system configuration as well as administrator and user logins and logouts. Activity events include system activities, such as VPN tunnel establishment and HA failover events. |
| <b>Virus Log</b>         | Record virus intrusion events, such as when the FortiGate unit detects a virus, blocks a file type, or blocks an oversized file or email.                                                                                                                                          |
| <b>Web Filtering Log</b> | Record activity events, such as URL and content blocking, and exemption of URLs from blocking.                                                                                                                                                                                     |
| <b>Attack Log</b>        | Record attacks detected by the NIDS and prevented by the NIDS Prevention module.                                                                                                                                                                                                   |

- Email Filter Log** Record activity events, such as detection of email that contains unwanted content and email from unwanted senders.
- Update** Record log messages when the FortiGate connects to the FDN to download antivirus and attack updates.
- 4 Select the message categories that you want the FortiGate unit to record if you selected Event Log, Virus Log, Web Filtering Log, Attack Log, Email Filter Log, or Update in step 3.
  - 5 Select OK.

Figure 43: Example log filter configuration

The screenshot shows the 'Local Log Filter' configuration window. The 'Traffic Filter' tab is selected. The window contains the following categories and options:

- ☐ **Traffic Log**
- ☐ **Event Log**
  - ☐ When configuration has changed
  - ☐ IPSec negotiation event
  - ☐ DHCP service event
  - ☐ PPP service event
  - ☐ Admin login/logout event
  - ☐ IP/MAC binding event
  - ☐ System activity event
  - ☐ HA activity event
  - ☐ Firewall authentication event
  - ☐ Route gateway event
- ☐ **Virus Log**
  - ☐ Virus infected
  - ☐ Filename blocked
  - ☐ File oversized
- ☐ **Web Filtering Log**
  - ☐ Content block
  - ☐ URL block
  - ☐ URL exempt
- ☐ **Attack Log**
  - ☐ Attack Detection
  - ☐ Attack Prevention
- ☐ **Email Filter Log**
  - ☐ Blocklist email detected
  - ☐ Banned word detected
- ☐ **Update**
  - ☐ Failed update
  - ☐ Successful update
  - ☐ FDN error

At the bottom of the window are 'OK' and 'Cancel' buttons.

## Configuring traffic logging

You can configure the FortiGate unit to record traffic log messages for connections to:

- Any interface
- Any firewall policy

The FortiGate unit can filter traffic logs for any source and destination address and service. You can also enable the following global settings:

- resolve IP addresses to host names,
- record session or packet information,
- display the port number or service.

The traffic filter list shows the name, source address and destination address, and the protocol type of the traffic to be filtered.

This section describes:

- [Enabling traffic logging](#)
- [Configuring traffic filter settings](#)
- [Adding traffic filter entries](#)

### Enabling traffic logging

You can enable logging on any interface and firewall policy.

#### Enabling traffic logging for an interface

If you enable traffic logging for an interface, all connections to and through the interface are recorded in the traffic log.

- 1 Go to **System > Network > Interface**.
- 2 Select Edit  in the Modify column beside the interface for which you want to enable logging.
- 3 For Log, select Enable.
- 4 Select OK.
- 5 Repeat this procedure for each interface for which you want to enable logging.

#### Enabling traffic logging for a firewall policy

If you enable traffic logging for a firewall policy, all connections accepted by firewall policy are recorded in the traffic log.

- 1 Go to **Firewall > Policy**.
- 2 Select a policy tab.
- 3 Select Log Traffic.
- 4 Select OK.

## Configuring traffic filter settings

Use the following procedure to configure the information recorded in all traffic log messages.

- 1 Go to **Log&Report > Log Setting > Traffic Filter**.

- 2 Select the settings that you want to apply to all Traffic Log messages.

- Resolve IP** Select Resolve IP if you want traffic log messages to list the IP address and the domain name stored on the DNS server. If the primary and secondary DNS server addresses provided to you by your ISP have not already been added, go to **System > Network > DNS** and add the addresses.
- Type** Select Session or Packet. If you select Session, the FortiGate unit records the number of packets sent and received for each session. If you select Packet, the FortiGate unit records the average packet length for each session (in bytes).
- Display** Select Port Number if you want traffic log messages to list the port number, for example, 80/tcp. Select Service Name if you want traffic log messages to list the name of the service, for example, TCP.

- 3 Select Apply.

Figure 44: Example traffic filter list

| Name                 | Source Address                | Destination Address         | Protocol | Modify  |
|----------------------|-------------------------------|-----------------------------|----------|---------|
| FTP_Main_Office      | 10.10.10.1/255.255.255.0      | 10.10.10.2/255.255.255.0    | FTP      | [Icons] |
| All_traffic          | 192.168.123.111/255.255.255.0 | 192.168.124.0/255.255.255.0 | ANY      | [Icons] |
| Email_Branch_to_Main | 10.10.11.0/255.255.255.0      | 10.10.10.0/255.255.255.0    | POP3     | [Icons] |

## Adding traffic filter entries

Add entries to the traffic filter list to filter the messages that are recorded in the traffic log. If you do not add any entries to the traffic filter list, the FortiGate records all traffic log messages. You can add entries to the traffic filter list to limit the traffic logs that are recorded. You can log traffic with a specified source IP address and netmask, to a destination IP address and netmask and for a specified service. A traffic filter entry can include any combination of source and destination addresses and services.

Use the following procedure to add an entry to the traffic filter list.

- 1 Go to **Log&Report > Log Setting > Traffic Filter**.
- 2 Select New.
- 3 Configure the traffic filter for the type of traffic that you want to record on the traffic log.

- Name** Type a name to identify the traffic filter entry. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and \_. Spaces and other special characters are not allowed.
- Source IP Address** Type the source IP address and netmask for which you want the FortiGate unit to log traffic messages. The address can be an individual computer, subnetwork, or network.
- Source Netmask**

**Destination IP Address** Type the destination IP address and netmask for which you want the FortiGate unit to log traffic messages. The address can be an individual computer, subnetwork, or network.

**Destination Netmask**

**Service** Select the service group or individual service for which you want the FortiGate unit to log traffic messages.

4 Select OK.

The traffic filter list displays the new traffic address entry with the settings that you selected in [“Enabling traffic logging” on page 253](#).

Figure 45: Example new traffic address entry

The screenshot shows the 'New Traffic' configuration window in the FortiGate web interface. The window has two tabs: 'Log Setting' and 'Traffic Filter'. The 'New Traffic' form contains the following fields and values:

| New Traffic                                                             |                 |
|-------------------------------------------------------------------------|-----------------|
| Name                                                                    | FTP_Main_Office |
| Source IP Address                                                       | 10.10.10.1      |
| Source Netmask                                                          | 255.255.255.0   |
| Destination IP Address                                                  | 10.10.10.2      |
| Destination Netmask                                                     | 255.255.255.0   |
| Service                                                                 | FTP             |
| <input type="button" value="OK"/> <input type="button" value="Cancel"/> |                 |

## Viewing logs saved to memory

If the FortiGate is configured to save log messages in system memory, you can use the web-based manager to view, search, and clear the log messages. This section describes:

- [Viewing logs](#)
- [Searching logs](#)

### Viewing logs

Log messages are listed with the most recent message at the top. Use the following procedure to view log messages saved in system memory:

- 1 Go to **Log&Report > Logging**.
- 2 Select Event Log, Attack Log, Antivirus Log, Web Filter Log, or Email Filter Log. The web-based manager lists the log messages saved in system memory.
- 3 Scroll through the log messages to view them.
- 4 To view a specific line in the log, type a line number in the Go to line field and select [Go](#).
- 5 To navigate through the log message pages, select Go to next page  or Go to previous page .

## Searching logs

Use the following procedure to search log messages saved in system memory:

- 1 Go to **Log&Report > Logging**.
- 2 Select Event Log, Attack Log, Antivirus Log, Web Filter Log, or Email Filter Log.
- 3 Select  to search the messages in the selected log.
- 4 Select AND to search for messages that match all the specified search criteria.
- 5 Select OR to search for messages that match one or more of the specified search criteria.
- 6 Select one or more of the following search criteria:
 

|                |                                                                                |
|----------------|--------------------------------------------------------------------------------|
| <b>Keyword</b> | To search for any text in a log message. Keyword searching is case-sensitive.  |
| <b>Time</b>    | To search log messages created during the selected year, month, day, and hour. |
- 7 Select OK to run the search.  
The web-based manager displays the messages that match the search criteria. You can scroll through the messages or run another search.



**Note:** After running a search, to display all log messages again, run another search but leave all the search fields blank.

## Configuring alert email

You can configure the FortiGate unit to send alert email to up to three email addresses when there are virus incidents, block incidents, network intrusions, and other firewall or VPN events or violations. After you set up the email addresses, you can test the settings by sending test email.

- [Adding alert email addresses](#)
- [Testing alert email](#)
- [Enabling alert email](#)

### Adding alert email addresses

Because the FortiGate unit uses the SMTP server name to connect to the mail server, it must be able to look up this name on your DNS server. Therefore, before configuring alert email ensure that you have configured at least one DNS server.

#### To add a DNS server

- 1 Go to **System > Network > DNS**.
- 2 If they have not already been added, add the primary and secondary DNS server addresses provided to you by your ISP.
- 3 Select Apply.

#### To add alert email addresses

- 1 Go to **Log&Report > Alert Mail > Configuration**.
- 2 Select Authentication if your email server requires an SMTP password.

- 3 In the SMTP Server field, type the name of the SMTP server to which the FortiGate unit should send email, in the format `smtp.domain.com`.  
The SMTP server can be located on any network connected to the FortiGate unit.
- 4 In the SMTP User field, type a valid email address in the format `user@domain.com`.  
This address appears in the From header of the alert email.
- 5 In the Password field, type the password that the SMTP user needs to access the SMTP server.  
A password is required if you select Authentication.
- 6 Type up to three destination email addresses in the Email To fields.  
These are the actual email addresses to which the FortiGate unit sends alert email.
- 7 Select Apply.

## Testing alert email

You can test the alert email settings by sending a test email.

- 1 Go to **Log&Report > Alert Mail > Configuration**.
- 2 Select Test to send test email messages from the FortiGate unit to the Email To addresses that you have configured.

## Enabling alert email

You can configure the FortiGate unit to send alert email in response to virus incidents, intrusion attempts, and critical firewall or VPN events or violations. If you have configured logging to a local disk, you can enable sending an alert email when the hard disk is almost full. Use the following procedure to enable alert email:

- 1 Go to **Log&Report > Alert Mail > Categories**.
- 2 Select Enable alert email for virus incidents to have the FortiGate unit send an alert email when antivirus scanning detects a virus.  
Alert email is not sent when antivirus file blocking deletes a file.
- 3 Select Enable alert email for block incidents to have the FortiGate unit send an alert email when it blocks files affected by viruses.
- 4 Select Enable alert email for intrusions to have the FortiGate unit send an alert email to notify the system administrator of attacks detected by the NIDS.
- 5 Select Enable alert email for critical firewall/VPN events or violations to have the FortiGate unit send an alert email when a critical firewall or VPN event occurs.  
Critical firewall events include failed authentication attempts.  
Critical VPN events include when replay detection detects a replay packet. Replay detection can be configured for both manual key and AutoIKE Key VPN tunnels.
- 6 Select Send alert email when disk is full to have the FortiGate unit send an alert email when the hard disk is almost full.
- 7 Select Apply.



# Glossary

**Connection:** A link between machines, applications, processes, and so on that can be logical, physical, or both.

**DMZ, Demilitarized Zone:** Used to host Internet services without allowing unauthorized access to an internal (private) network. Typically, the DMZ contains servers accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (email) servers and DNS servers.

**DMZ interface:** The FortiGate interface that is connected to a DMZ network.

**DNS, Domain Name Service:** A service that converts symbolic node names to IP addresses.

**Ethernet:** A local-area network (LAN) architecture that uses a bus or star topology and supports data transfer rates of 10 Mbps. Ethernet is one of the most widely implemented LAN standards. A newer version of Ethernet, called 100 Base-T (or Fast Ethernet), supports data transfer rates of 100 Mbps. And the newest version, Gigabit Ethernet, supports data rates of 1 gigabit (1,000 megabits) per second.

**External interface:** The FortiGate interface that is connected to the Internet. For the FortiGate-60 the external interface is WAN1 or WAN2.

**FTP, File transfer Protocol:** An application and TCP/IP protocol used to upload or download files.

**Gateway:** A combination of hardware and software that links different networks. Gateways between TCP/IP networks, for example, can link different subnetworks.

**HTTP, Hyper Text Transfer Protocol:** The protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

**HTTPS:** The SSL protocol for transmitting private documents over the Internet using a Web browser.

**Internal interface:** The FortiGate interface that is connected to an internal (private) network.

**Internet:** A collection of networks connected together that span the entire globe using the NFNET as their backbone. As a generic term, it refers to any collection of interdependent networks.

**ICMP, Internet Control Message Protocol:** Part of the Internet Protocol (IP) that allows for the generation of error messages, test packets, and information messages relating to IP. This is the protocol used by the ping function when sending ICMP Echo Requests to a network host.

**IKE, Internet Key Exchange:** A method of automatically exchanging authentication and encryption keys between two secure servers.

**IMAP, Internet Message Access Protocol:** An Internet email protocol that allows access to your email from any IMAP compatible browser. With IMAP, your mail resides on the server.

**IP, Internet Protocol:** The component of TCP/IP that handles routing.

**IP Address:** An identifier for a computer or device on a TCP/IP network. An IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255.

**L2TP, Layer Two (2) Tunneling Protocol:** An extension to the PPTP protocol that enables ISPs to operate Virtual Private Networks (VPNs). L2TP merges PPTP from Microsoft and L2F from Cisco Systems. To create an L2TP VPN, your ISP's routers must support L2TP.

**IPSec, Internet Protocol Security:** A set of protocols that support secure exchange of packets at the IP layer. IPSec is most often used to support VPNs.

**LAN, Local Area Network:** A computer network that spans a relatively small area. Most LANs connect workstations and personal computers. Each computer on a LAN is able to access data and devices anywhere on the LAN. This means that many users can share data as well as physical resources such as printers.

**MAC address, Media Access Control address:** A hardware address that uniquely identifies each node of a network.

**MIB, Management Information Base:** A database of objects that can be monitored by an SNMP network manager.

**Modem:** A device that converts digital signals into analog signals and back again for transmission over telephone lines.

**MTU, Maximum Transmission Unit:** The largest physical packet size, measured in bytes, that a network can transmit. Any packets larger than the MTU are divided into smaller packets before being sent. Ideally, you want the MTU your network produces to be the same as the smallest MTU of all the networks between your machine and a message's final destination. If your messages are larger than one of the intervening MTUs, they get broken up (fragmented), which slows down transmission speeds.

**Netmask:** Also called subnet mask. A set of rules for omitting parts of a complete IP address to reach a target destination without using a broadcast message. It can indicate a subnetwork portion of a larger network in TCP/IP. Sometimes referred to as an Address Mask.

**NTP, Network Time Protocol:** Used to synchronize the time of a computer to an NTP server. NTP provides accuracies to within tens of milliseconds across the Internet relative to Coordinated Universal Time (UTC).

**Packet:** A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

**Ping, Packet Internet Grouper:** A utility used to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply.

**POP3, Post Office Protocol:** A protocol used to transfer e-mail from a mail server to a mail client across the Internet. Most e-mail clients use POP.

**PPP, Point-to-Point Protocol:** A TCP/IP protocol that provides host-to-network and router-to-router connections.

**PPTP, Point-to-Point Tunneling Protocol:** A Windows-based technology for creating VPNs. PPTP is supported by Windows 98, 2000, and XP. To create a PPTP VPN, your ISP's routers must support PPTP.

**Port:** In TCP/IP and UDP networks, a port is an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

**Protocol:** An agreed-upon format for transmitting data between two devices. The protocol determines the type of error checking to be used, the data compression method (if any), how the sending device indicates that it has finished sending a message, and how the receiving device indicates that it has received a message.

**RADIUS, Remote Authentication Dial-In User Service:** An authentication and accounting system used by many Internet Service Providers (ISPs). When users dial into an ISP they enter a user name and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

**Router:** A device that connects LANs into an internal network and routes traffic between them.

**Routing:** The process of determining a path to use to send data to its destination.

**Routing table:** A list of valid paths through which data can be transmitted.

**Server:** An application that answers requests from other devices (clients). Used as a generic term for any device that provides services to the rest of the network such as printing, high capacity storage, and network access.

**SMTP, Simple Mail Transfer Protocol:** In TCP/IP networks, this is an application for providing mail delivery services.

**SNMP, Simple Network Management Protocol:** A set of protocols for managing networks. SNMP works by sending messages to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

**SSH, Secure shell:** A secure Telnet replacement that you can use to log into another computer over a network and run commands. SSH provides strong secure authentication and secure communications over insecure channels.

**Subnet:** A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 100.100.100. would be part of the same subnet. Dividing a network into subnets is useful for both security and performance reasons. IP networks are divided using a subnet mask.

**Subnet Address:** The part of the IP address that identifies the subnetwork.

**TCP, Transmission Control Protocol:** One of the main protocols in TCP/IP networks. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

**UDP, User Datagram Protocol:** A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP, UDP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It is used primarily for broadcasting messages over a network.

**VPN, Virtual Private Network:** A network that links private networks over the Internet. VPNs use encryption and other security mechanisms to ensure that only authorized users can access the network and that data cannot be intercepted.

**Virus:** A computer program that attaches itself to other programs, spreading itself through computers or networks by this mechanism usually with harmful intent.

**Worm:** A program or algorithm that replicates itself over a computer network, usually through email, and performs malicious actions, such as using up the computer's resources and possibly shutting the system down.



# Index

## A

- accept
  - policy 145
- action
  - policy option 145
- active log
  - searching 256
- ActiveX 242
  - removing from web pages 242
- address 150
  - adding 151
  - editing 152
  - group 152
  - IP/MAC binding 167
  - virtual IP 160
- address group 152
  - example 153
- address name 151
- admin access level
  - administrator account 132
- administrator account
  - adding 132
  - admin 132
  - changing password 133
  - editing 132, 133
  - netmask 132, 133
  - permission 133
  - trusted host 132, 133
- alert email
  - configuring 256
  - configuring SMTP server 257
  - content of messages 229
  - critical firewall or VPN events 257
  - enabling 257
  - hard disk full 257
  - intrusion attempts 257
  - reducing messages 224
  - testing 257
  - virus incidents 257
- allow inbound
  - encrypt policy 146
- allow outbound
  - encrypt policy 146
- allow traffic
  - IP/MAC binding 167
- Anti-Virus & Web filter
  - policy 147
- antivirus definition updates
  - manual 82
- antivirus definitions
  - updating 91
- antivirus updates 93
  - configuring 94
  - through a proxy server 100
- attack definition updates
  - downloading 106, 107
  - manual 83
- attack definitions
  - updating 91, 95
- attack detection
  - checksum verification 222
  - disabling the NIDS 222
  - enabling and disabling signatures 224
  - selecting interfaces to monitor 222
  - viewing the signature list 223
- attack log 251
  - content of messages 229
  - reducing messages 224
- attack prevention
  - configuring signature threshold values 226
  - enabling prevention signatures 225
  - NIDS 225
- attack updates
  - configuring 94
  - scheduling 93
  - through a proxy server 100
- authentication 147, 173
  - configuring 174
  - enabling 179
  - LDAP server 177
  - RADIUS server 176
  - timeout 131
- auto
  - device in route 117
- AutoIKE 182
  - certificates 182
  - introduction 182
  - pre-shared keys 182
- automatic antivirus and attack definition updates
  - configuring 94

**B**

- backing up
  - system settings 83
- bandwidth
  - guaranteed 146
  - maximum 146
- banned word list
  - adding words 236, 246
- blacklist
  - URL 239
- block traffic
  - IP/MAC binding 167
- blocking
  - access to Internet sites 237, 247
  - access to URLs 237, 247
  - adding filename patterns 233
  - file 233
  - oversized files and email 234
  - web pages 236, 246

**C**

- certificates
  - introduction 182
- checksum verification
  - configuring 222
- clearing
  - communication sessions 89
  - URL block list 238
- CLI 18
  - configuring IP addresses 45, 59
  - configuring NAT/Route mode 45
  - connecting to 31
  - upgrading the firmware 71, 73
- command line interface 18
- Comments
  - firewall policy 148
  - policy 148
- connecting
  - to the FDN 92
  - to the FortiResponse Distribution Network 92
  - to your network 47, 60
  - web-based manager 30, 45
- contact information
  - registration 106
  - SNMP 134
- content blocking
  - exempting URLs 243, 247
  - web page 236, 246
- content filter 235, 245
- content profiles
  - default 170
- cookies
  - blocking 242
- critical firewall events
  - alert email 257
- critical VPN events
  - alert email 257

- custom service 156
- customer service 25

**D**

- date and time setting
  - example 130, 137
- date setting 129
- default gateway
  - configuring (Transparent mode) 59
- default route 119
- deny
  - firewall policy 145
  - policy 145
- destination
  - policy option 145
- destination route
  - adding 116
  - adding a default route 116
- detection
  - NIDS 221
- device
  - auto 117
- DHCP
  - ending IP address 119
  - external interface 112
  - internal network 119
  - internal network settings 120
  - WINS 119
- dialup L2TP
  - configuring Windows 2000 client 217
  - configuring Windows XP client 218
- dialup PPTP
  - configuring Windows 2000 client 211
  - configuring Windows 98 client 210
  - configuring Windows XP client 212
- dialup VPN
  - viewing connection status 205
- disabling NIDS 222
- DMZ interface
  - configuring 48
  - definition 259
- DNS
  - server addresses 115
- DNS IP
  - DHCP setting 119
- domain
  - DHCP 119
- downloading
  - attack definition updates 106, 107
  - virus definition updates 106, 107
- dynamic IP list
  - viewing 120
- dynamic IP pool
  - IP pool 146
- dynamic IP/MAC list 166
  - viewing 168

## E

- email alert
  - testing 257
- email filter log 252
- enabling policy 150
- encrypt
  - policy 145
- encrypt policy
  - allow inbound 146
  - allow outbound 146
  - Inbound NAT 146
  - Outbound NAT 146
- ending IP address
  - DHCP 119
  - PPTP 208, 214
- environmental specifications 29
- event log 251
  - viewing 255
- exclusion range
  - DHCP 119
- exempt URL list 243, 247
  - adding URL 243, 248
- exempting URLs from content and URL blocking 243, 247
- expire
  - system status 90
- external interface
  - configuring DHCP 112
  - configuring PPPoE 113

## F

- factory default
  - restoring system settings 84
- FAQs 205
- FDN
  - connecting to 92
  - FortiResponse Distribution Network 92
- FDS
  - FortiResponse Distribution Server 92
- filename pattern
  - adding 233
  - blocking 233
- filter
  - RIP 126
- filtering log messages 251
- filtering traffic 253
- firewall
  - authentication timeout 131
  - configuring 141
  - introduction 15
  - overview 141
- firewall events
  - enabling alert email 257

- firewall policy
  - accept 145
  - Comments 148
  - deny 145
  - guaranteed bandwidth 146
  - Log Traffic 148
  - maximum bandwidth 146
- firewall setup wizard 18, 45, 58
  - starting 45, 58
- firmware
  - changing 70
  - installing 75
  - re-installing current version 75
  - reverting to an older version 75
  - upgrading 70
  - upgrading to a new version 71
  - upgrading using the CLI 71, 73
  - upgrading using the web-base manager 71, 72
- first trap receiver IP address
  - SNMP 135
- fixed port 146
- FortiCare
  - service contracts 101
  - support contract number 105
- Fortinet customer service 25
- Fortinet support
  - recovering a lost password 104
- FortiResponse Distribution Network 92
  - connecting to 92
- FortiResponse Distribution Server 92
- from IP
  - system status 89
- from port
  - system status 89

## G

- get community
  - SNMP 134
- grouping services 156
- groups
  - address 152
  - user 179
- guaranteed bandwidth 146

## H

- hard disk full
  - alert email 257
- HTTP
  - enabling web filtering 235, 245
- HTTPS 17, 154, 259

## I

- ICMP 155, 259
  - configuring checksum verification 222
- idle timeout
  - web-based manager 130

- IDS log
  - viewing 255
- IKE 259
- IMAP 154, 259
- Inbound NAT
  - encrypt policy 146
- interface
  - RIP 124
- internal address
  - example 152
- internal address group
  - example 153
- internal network
  - configuring 48
- Internet
  - blocking access to Internet sites 237, 247
  - blocking access to URLs 237, 247
- Internet key exchange 259
- intrusion attempts
  - alert email 257
- IP
  - configuring checksum verification 222
- IP address
  - IP/MAC binding 166
- IP addresses
  - configuring from the CLI 45, 59
- IP pool
  - adding 164
- IP spoofing 166
- IP/MAC binding 166
  - adding 167
  - allow traffic 167
  - block traffic 167
  - dynamic IP/MAC list 166
  - enabling 168
  - static IP/MAC list 166
- IPSec 259
- IPSec VPN
  - authentication for user group 179
  - AutoIKE 182
  - certificates 182
  - disabling 217, 219
  - manual keys 182
  - pre-shared keys 182
  - remote gateway 179
  - status 205
  - timeout 205, 206
- IPSec VPN tunnel
  - testing 206

## J

- Java applets 242
  - removing from web pages 242

## K

- keyword
  - log search 256

## L

- L2TP 179, 259
  - configuring Windows XP client 218
  - network configuration 214
- L2TP gateway
  - configuring 214
- language
  - web-based manager 131
- LDAP
  - example configuration 178
- LDAP server
  - adding server address 177
  - deleting 178
- lease duration
  - DHCP 119
- log setting
  - filtering log entries 94, 251
  - traffic filter 254
- log to memory
  - configuring 251
  - viewing saved logs 255
- Log Traffic
  - firewall policy 148
  - policy 148
- logging 19, 249
  - attack log 251
  - configuring traffic settings 253, 254
  - email filter log 252
  - enabling alert email 257
  - event log 251
  - filtering log messages 251
  - log to memory 251
  - log to remote host 250
  - log to WebTrends 250
  - recording 249
  - searching logs 256
  - selecting what to log 251
  - traffic log 251
  - traffic sessions 253
  - update log 252
  - virus log 251
  - web filtering log 251
- logs
  - recording on NetIQ WebTrends server 250

## M

- MAC address 260
  - IP/MAC binding 166
- malicious scripts
  - removing from web pages 242, 248
- management interface
  - Transparent mode 114
- management IP address
  - transparent mode 59
- manual keys
  - introduction 182
- matching
  - policy 149

- maximum bandwidth 146
- messages
  - replacement 135
- MIB
  - FortiGate 135
- mode
  - Transparent 16
- monitor
  - system status 86, 87, 88, 89
- monitored interfaces 222
- MTU size 113
  - changing 113
  - definition 260
  - improving network performance 113

## N

- NAT
  - introduction 15
  - policy option 145
  - push updates 96
- NAT mode
  - adding policy 144
  - IP addresses 45
- NAT/Route mode
  - configuration from the CLI 45
  - introduction 15
- neighbor
  - RIP 125
- netmask
  - administrator account 132, 133
- network address translation
  - introduction 15
- network configuration
  - changing 109
- network intrusion detection 16
- Network Intrusion Detection System 221
- next hop router 111
- NIDS 16, 221
  - attack prevention 225
  - detection 221
  - prevention 225
  - reducing alert email 229
  - reducing attack log messages 229
  - user-defined signatures 224
- NTP 48, 61, 155, 260
- NTP server 129
  - setting system date and time 129

## O

- one-time schedule 158
  - creating 158
- operating mode
  - changing 85
- Outbound NAT
  - encrypt policy 146
- override serve
  - adding 94, 95

- oversized files and email
  - blocking 234

## P

- password
  - adding 174
  - changing administrator account 133
  - Fortinet support 106
  - recovering a lost Fortinet support 104
- PAT 161
- permission
  - administrator account 133
- policy
  - accept 145
  - Anti-Virus & Web filter 147
  - arranging in policy list 149
  - Comments 148
  - deny 145
  - disabling 150
  - enabling 150
  - enabling authentication 179
  - fixed port 146
  - guaranteed bandwidth 146
  - Log Traffic 148
  - matching 149
  - maximum bandwidth 146
- policy list
  - configuring 149
- policy routing 118
- POP3 155, 260
- port address translation 161
- port forwarding 161
  - adding virtual IP 161
  - virtual IP 160
- port number
  - traffic filter display 254
- power requirements 28
- powering on 29
- PPPoE
  - external interface 113
- PPTP 179, 260
  - configuring gateway 208, 214
  - configuring Windows 2000 client 211
  - configuring Windows 98 client 210
  - configuring Windows XP client 212
  - enabling 208, 214
  - ending IP address 208, 214
  - network configuration 208
  - starting IP 208, 214
- PPTP dialup connection
  - configuring Windows 2000 client 211
  - configuring Windows 98 client 211
  - configuring Windows XP client 212
- PPTP gateway
  - configuring 208
- predefined services 153
- pre-shared keys
  - introduction 182

- prevention
  - NIDS 225
- protocol
  - service 154
  - system status 89
- proxy server 100
  - push updates 100
- push updates
  - configuring 95
  - through a NAT device 96
  - through a proxy server 100
- R**
- RADIUS
  - definition 260
  - example configuration 176
- RADIUS server
  - adding server address 176
  - deleting 176
- read & write access level
  - administrator account 132
- read only access level
  - administrator account 132
- recording logs 249
- recording logs in system memory 251
- recording logs on NetIQ WebTrends server 250
- recovering
  - a lost Fortinet support password 104
- recurring schedule 159
  - creating 158
- registered FortiGate units
  - viewing the list of 104
- registering
  - FortiGate unit 101, 102, 103, 105
  - FortiGate unit after an RMA 107
  - list of registered FortiGate units 105
- registration
  - contact information 106
  - security question 106
  - updating information 104
- replacement messages
  - customizing 135
- reporting 19, 249
- resolve IP 254
  - traffic filter 254
- restarting 85
- restoring system settings 84
- restoring system settings to factory default 84
- reverting
  - firmware to an older version 75
- RIP
  - configuring 121
  - filters 126
  - interface configuration 124
  - neighbors 125
  - settings 122
- RMA
  - registering a FortiGate unit 107

- route
  - adding default 116
  - adding to routing table 116
  - adding to routing table (Transparent mode) 117
  - destination-based 116
  - device 117
- router
  - next hop 111
- routing 260
  - adding static routes 116
  - configuring 115
  - configuring routing table 118
  - policy 118
- routing table 260
  - adding default route 116
  - adding routes 116
  - adding routes (Transparent mode) 117
  - configuring 118
- S**
- scanning
  - antivirus 232
- schedule 157
  - applying to policy 159
  - automatic antivirus and attack definition updates 93
  - creating one-time 158
  - creating recurring 158
  - one-time 158
  - policy option 145
  - recurring 159
- scheduled antivirus and attack updates 100
- scheduled updates
  - through a proxy server 100
- scheduling 93
- script filter 242
  - example settings 242
- scripts
  - removing from web pages 242, 248
- searching logs 256
  - logs saved to memory 255
- security question
  - registration 106
- serial number
  - displaying 83
- service 153
  - custom 156
  - group 156
  - policy option 145
  - predefined 153
  - service name 154
  - user-defined 156
- service contracts
  - Forticare 101
- service group
  - adding 157
- service name
  - traffic filter display 254

- session
  - clearing 89
- set time 129
- setup wizard 45, 58
  - starting 45, 58
- shutting down 86
- signature threshold values 226
- SMTP 155
  - configuring alert email 257
  - definition 260
- SNMP
  - configuring 134
  - contact information 134
  - definition 260
  - first trap receiver IP address 135
  - get community 134
  - MIBs 135
  - system location 134
  - trap community 135
  - traps 136
- source
  - policy option 145
- squidGuard 239
- SSH 155, 261
- SSL 259
  - service definition 154
- starting IP
  - DHCP 119
  - PPTP 208, 214
- static IP/MAC list 166
- static NAT virtual IP 160
  - adding 160
- static route
  - adding 116
- status
  - IPSec VPN tunnel 205
  - viewing dialup connection status 205
  - viewing VPN tunnel status 205
- subnet
  - definition 261
- subnet address
  - definition 261
- support contract number
  - adding 105
  - changing 105
- support password
  - changing 106
- syn interval 130
- synchronize with NTP server 129
- system configuration 129
- system date and time
  - setting 129
- system location
  - SNMP 134
- system name
  - SNMP 134

- system settings
  - backing up 83
  - restoring 84
  - restoring to factory default 84
- system status 69, 121
- system status monitor 86, 87, 88, 89

## T

- TCP
  - configuring checksum verification 222
- technical support 25
- testing
  - alert email 257
- time
  - log search 256
  - setting 129
- time zone 129
- timeout
  - firewall authentication 131
  - idle 130
  - IPSec VPN 205, 206
  - web-based manager 130
- to IP
  - system status 90
- to port
  - system status 90
- traffic
  - configuring global settings 253, 254
  - filtering 253
  - logging 253
- traffic filter
  - adding entries 254
  - display 254
  - log setting 254
  - packet 254
  - port number 254
  - resolve IP 254
  - service name 254
  - session 254
  - type 254
- traffic log 251
- Traffic Priority 146
- Traffic Shaping 146
- Transparent mode 16
  - adding routes 117
  - changing to 59
  - configuring the default gateway 59
  - management interface 114
  - management IP address 59
- trap community
  - SNMP 135
- traps
  - SNMP 136
- troubleshooting 205
- trusted host
  - administrator account 132, 133

**U**

- UDP
  - configuring checksum verification 222
- unwanted content
  - blocking 236, 246
- update 252
  - attack 94
  - push 95
- updated
  - antivirus 94
- updating
  - attack definitions 91, 95
  - virus definitions 91, 95
- upgrade
  - firmware 71
- upgrading
  - firmware 70
  - firmware using the CLI 71, 73
  - firmware using the web-based manager 71, 72
- URL
  - adding to exempt URL list 243, 248
  - adding to URL block list 237, 247
  - blocking access 237, 247
- URL block list
  - adding URL 237, 247
  - clearing 238
  - downloading 239
  - uploading 239
- URL block message 236
- URL blocking
  - exempt URL list 243, 247
- URL exempt list
  - see also exempt URL list 243, 247
- user authentication 173
- user groups
  - configuring 179
  - deleting 180
- user name and password
  - adding 175
  - adding user name 174
- user-defined services 156
- user-defined signature
  - NIDS 224

**V**

- viewing
  - dialup connection status 205
  - logs saved to memory 255
  - VPN tunnel status 205
- virtual IP 160
  - adding 160
  - port forwarding 160, 161
  - static NAT 160
- virus definition updates
  - downloading 106, 107
- virus definitions
  - updating 91, 95
- virus incidents
  - enabling alert email 257
- virus list
  - displaying 234
  - viewing 234
- virus log 251
- virus protection
  - overview 231
  - worm protection 13
- VPN
  - configuring L2TP gateway 214
  - configuring PPTP gateway 208, 214
  - introduction 16
  - L2TP configuration 214
  - PPTP configuration 208
  - Tunnel 146
  - viewing dialup connection status 205
- VPN events
  - enabling alert email 257
- VPN tunnel
  - viewing status 205

**W**

- web content filtering
  - introduction 14
- web filtering
  - ActiveX 242
  - cookies 242
  - Java applets 242
  - overview 235, 245
- web filtering log 251
- web page
  - content blocking 236, 246
- web-based manager 18
  - changing options 130
  - connecting to 30, 45
  - introduction 17
  - language 131
  - timeout 130
- WebTrends
  - recording logs on NetIQ WebTrends server 250
- Windows 2000
  - configuring for L2TP 217
  - configuring for PPTP 211
  - connecting to L2TP VPN 218
  - connecting to PPTP VPN 212
- Windows 98
  - configuring for PPTP 210
  - connecting to PPTP VPN 211
- Windows XP
  - configuring for L2TP 218
  - configuring for PPTP 212
  - connecting to L2TP VPN 220
  - connecting to PPTP VPN 213
- WINS
  - DHCP server 119

|                       |                     |
|-----------------------|---------------------|
| wizard                | worm list           |
| firewall setup 45, 58 | displaying 234      |
| starting 45, 58       | worm protection 234 |

